



"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

## MESA DIRECTIVA

PODER LEGISLATIVO FEDERAL  
COMISIÓN PERMANENTE

OFICIO No. CP2R2A.-1239

Ciudad de México, 8 de julio de 2020

**DIP. JUANITA GUERRA MENA**  
**PRESIDENTA DE LA COMISIÓN DE**  
**SEGURIDAD PÚBLICA**  
**P R E S E N T E**

Me permito comunicar a Usted que en sesión celebrada en esta fecha, el Diputado Moisés Ignacio Mier Velazco, del Grupo Parlamentario Morena, presentó Iniciativa con proyecto de decreto por el que se expide la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública, y se reforman y adicionan diversas disposiciones de la Ley General del Sistema Nacional de Seguridad Pública; de la Ley del Sistema Nacional de Información Estadística y Geográfica; de la Ley de la Guardia Nacional; de la Ley Orgánica de la Fiscalía General de la República; de la Ley Federal de Telecomunicaciones y Radiocomunicación; y de la Ley General de Protección Civil.

La Presidencia, con fundamento en los artículos 21, fracción III y 179 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, dispuso que dicha Iniciativa, misma que se anexa, se turnara a la Comisión de Seguridad Pública, con opinión de la Comisión de Presupuesto y Cuenta Pública de la Cámara de Diputados.

Atentamente

**DIP. SERGIO CARLOS GUTIÉRREZ LUNA**  
**Secretario**





"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

PODER LEGISLATIVO FEDERAL  
COMISIÓN PERMANENTE

## MESA DIRECTIVA

**OFICIO No. CP2R2A.-1240**

Ciudad de México, 8 de julio de 2020

**DIP. ERASMO GONZÁLEZ ROBLEDO**  
**PRESIDENTE DE LA COMISIÓN DE**  
**PRESUPUESTO Y CUENTA PÚBLICA**  
**P R E S E N T E**

Me permito comunicar a Usted que en sesión celebrada en esta fecha, el Diputado Moisés Ignacio Mier Velazco, del Grupo Parlamentario Morena, presentó Iniciativa con proyecto de decreto por el que se expide la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública, y se reforman y adicionan diversas disposiciones de la Ley General del Sistema Nacional de Seguridad Pública; de la Ley del Sistema Nacional de Información Estadística y Geográfica; de la Ley de la Guardia Nacional; de la Ley Orgánica de la Fiscalía General de la República; de la Ley Federal de Telecomunicaciones y Radiocomunicación; y de la Ley General de Protección Civil.

La Presidencia, con fundamento en los artículos 21, fracción III y 179 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, dispuso que dicha Iniciativa, misma que se anexa, se turnara a la Comisión de Seguridad Pública, con opinión de la Comisión de Presupuesto y Cuenta Pública de la Cámara de Diputados.



Atentamente

**DIP. SERGIO CARLOS GUTIÉRREZ LUNA**  
**Secretario**

08 JUL 2020 se turnó a la Comisión de Seguridad Pública, con  
opinión de la Comisión de Presupuesto y Cuenta Pública de la  
Cámara de Diputados  
**Iniciativa con proyecto de decreto que expide la Ley Nacional del Sistema  
Nacional de la Información y Comunicaciones para la Seguridad Pública, y se  
reforman y adicionan diversas disposiciones de la Ley General del Sistema  
Nacional de Seguridad Pública; de la Ley del Sistema Nacional de Información  
Estadística y Geográfica; de la Ley de la Guardia Nacional; de la Ley Orgánica  
de la Fiscalía General de la República; de la Ley Federal de  
Telecomunicaciones y Radiocomunicación; y de la Ley General de Protección  
Civil.**

69

El que suscribe, el Diputado Moisés Ignacio Mier Velazco, integrante del Grupo Parlamentario MORENA, en la LXIV Legislatura del Congreso de la Unión, con fundamento en lo dispuesto por los artículos 71, fracción II y 78 fracción III, de la Constitución Política de los Estados Unidos Mexicanos, y en los artículos 55, fracción II, y 179 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos.

### **Exposición de Motivos**

El artículo 21, párrafo 9 de la Constitución Política de los Estados Unidos Mexicanos establece que “La seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz<sup>1</sup>...”. Asimismo, el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, en su enciclopedia jurídica mexicana, señala que la Seguridad Pública es “la actividad encomendada al Estado, para salvaguardar los intereses de la sociedad, los cuales se definirán técnicamente como bienes jurídicos, en actividades de prevención y como presupuesto de una debida procuración y administración de justicia”.

Para los efectos anteriores, el Estado ha creado el Sistema Nacional de Seguridad Pública que regula la Ley Nacional de la materia y conforme a ésta, establece en su artículo 2 que la seguridad pública “comprende la prevención especial y general de los delitos, la sanción de las infracciones administrativas, así como la investigación y la persecución de los delitos y la reinserción social del sentenciado<sup>2</sup>”.

Conforme al artículo 3 de la misma ley “la función de seguridad pública se realizará en los diversos ámbitos de competencia por conducto de las instituciones policiacas, de procuración de justicia, de las instancias encargadas de aplicar las infracciones administrativas, de la supervisión de medidas cautelares, de suspensión condicional

<sup>1</sup> [http://www.diputados.gob.mx/LeyesBiblio/pdf/1\\_080520.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf)

<sup>2</sup> [http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP\\_270519.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP_270519.pdf)

del procedimiento de los responsables de la prisión preventiva y ejecución de penas, así como por las demás autoridades que en razón de sus atribuciones deben contribuir directa e indirectamente al objeto de esta ley<sup>3</sup>.

En general, puede afirmarse que la seguridad pública comprende en esencia, la prevención del delito, el combate al crimen y la procuración de la justicia.

En nuestro país, la criminalidad ha tenido un elevado crecimiento en los últimos años por razones de carácter multifactorial, sin embargo, en el corto plazo cercano, medido de los años 2015 al 2019, ese crecimiento se ha pronunciado como se aprecia en el cuadro siguiente<sup>4</sup>:

<b>NÚMERO DE DELITOS DEL FUERO</b>	<b>2015</b>	<b>2016</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>
<b>FEDERAL</b>	95,727	85,213	96,035	112,917	98,396
<b>COMÚN</b>	1,536,483	1,658,550	1,939,497	1,989,930	2,038,951
<b>TOTAL</b>	<b>1,632,210</b>	<b>1,743,763</b>	<b>2,035,532</b>	<b>2,102,847</b>	<b>2,137,347</b>

Fuente: elaboración propia con datos del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública<sup>5</sup>.

Del cuadro se desprende que el **crecimiento** que ha tenido la **incidencia delictiva** alcanzó un **30.9%**, correspondiendo en promedio al fuero común un aumento de **32.7%** y al fuero federal del **2.8%**.

En particular, considerando el acumulado de ambos fueros, en el periodo de 2015 a 2019, los principales delitos han tenido los siguientes crecimientos:

<b>DELITOS</b>	<b>2015</b>	<b>2019</b>	<b>INCREMENTO</b>	<b>%</b>
<b>Contra la vida y la integridad</b>				
Feminicidio	411	983	572	139
Homicidio doloso	16,121	29,421	13,300	82.5
Lesiones dolosas	139,783	164,143	24,360	17.4
<b>Contra la libertad personal</b>				
Libertad personal (secuestro, tráfico de menores, rapto y otros)	12,281	21,853	9572	77.9
<b>Contra la libertad y la seguridad sexual</b>				

<sup>3</sup> [http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP\\_270519.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP_270519.pdf)

<sup>4</sup> <https://www.gob.mx/sesnsp/acciones-y-programas/incidencia-delictiva-del-fuero-comun-nueva-metodologia?state=published>

<sup>5</sup> <https://www.gob.mx/sesnsp/acciones-y-programas/incidencia-delictiva-del-fuero-federal?idiom=es>

Libertad y seguridad sexual (Abuso sexual, acoso sexual, hostigamiento sexual, violación simple, violación equiparada, incesto y otros)	31,171	51,662	20,491	<b>65.7</b>
<b>Contra el patrimonio</b>				
Fraude	57,417	75,433	18,016	<b>31.4</b>
Robo en todas sus modalidades	578,401	758,032	179,631	<b>31.1</b>
Daño a la propiedad	114,864	133,314	18,450	<b>16.1</b>
<b>Contra la familia</b>				
Violencia familiar	126,816	204,128	77,312	<b>61.0</b>
<b>Contra la sociedad</b>				
La sociedad (Corrupción de menores, trata de personas y otros)	4,721	9,613	4,892	<b>103.6</b>
<b>Contra otros bienes</b>				
Narcomenudeo	41,543	71,606	30,063	<b>72.4</b>
Amenazas	68,007	107,886	39,879	<b>58.6</b>
Otros	201,692	229,468	27,776	<b>13.8</b>
Contra la salud	9,255	7,737	1,518	<b>16.4</b>
Otros federales	60,406	65,963	5,557	<b>9.2</b>

Fuente: elaboración propia con datos del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública<sup>6</sup>.

Año 2015<sup>7</sup>.

Año 2019<sup>8</sup>.

Por otra parte, en el país se cuentan con 119 complejos de seguridad que recibieron, según datos del Sistema Nacional de Seguridad Pública, 95.02 millones de llamadas de emergencia, sin embargo, el 83% de éstas fueron improcedentes, cerca de 79 millones.

El mismo artículo 21 de la Constitución en su párrafo 10 inciso b), señala que “El establecimiento de un Sistema Nacional de Información en Seguridad Pública a cargo de la Federación al que ésta, las entidades federativas y los Municipios, a través de las dependencias responsables de la seguridad pública, proporcionarán la información de que dispongan en la materia, conforme a la ley”<sup>9</sup>.

El Sistema Nacional de Información se sustenta en el uso de recursos de tecnología, en particular de Tecnologías de la Información y Comunicaciones, para lo cual se requiere de una total coordinación entre las diversas plataformas de sistemas de información de las entidades federativas y municipios, que permitan fortalecer el acopio, análisis y procesamiento de la información en materia de seguridad pública.

<sup>6</sup><https://www.gob.mx/sesnsp/acciones-y-programas/incidencia-delictiva-del-fuero-comun-nueva-metodologia?state=published>

<sup>7</sup> <https://drive.google.com/file/d/1RQhk58-fHNPrft2OaDFk8adUqP0fqOm/view>

<sup>8</sup> [https://drive.google.com/file/d/17MnLmvY\\_YW5ZbyHle5n5ROkWdPNNFIWT/view](https://drive.google.com/file/d/17MnLmvY_YW5ZbyHle5n5ROkWdPNNFIWT/view)

<sup>9</sup> [http://www.diputados.gob.mx/LeyesBiblio/pdf/1\\_080520.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf)

La información a que se refiere la disposición constitucional que establece la instauración de un “sistema nacional de información en seguridad pública”, guarda una relación directa con los servicios que prestan los Complejos de Seguridad, operados por las entidades federativas y con las bases de datos criminalísticas operados por Plataforma México dependiente de la Secretaría de Seguridad y protección Ciudadana.

Los principales servicios que proporcionan esos Complejos: la atención de llamadas de emergencia 9-1-1, los sistemas de video vigilancia y la atención y control de tecnologías emergentes —alarmas, botones de pánico, sistemas de rastreo vehicular, aplicaciones ciudadanas de voz, datos e imágenes e incluso drones— están soportados básicamente por las Tecnologías de la Información y Comunicaciones (TIC).

Esos servicios, desde luego apoyan la prevención de los delitos, el combate a los mismos a través de los servicios policiacos y de investigación, es decir, soportan en buena medida también el combate al crimen, la procuración de justicia y demás servicios de seguridad pública. En suma, los servicios de los Complejos de Seguridad dan un soporte científico y práctico a la seguridad pública.

Los servicios a que se ha hecho referencia están soportados fundamentalmente por las Tecnologías de la Información y Comunicaciones que están constituidas por un conjunto de procesos y productos que son el resultado del empleo de nuevas herramientas surgidas del campo de la informática, soporte de la información y canales de comunicación, relacionados con el almacenamiento, procesamiento y transmisión digital de la información. En el ámbito de la seguridad pública, resultan primordiales como herramientas a ser incorporadas en el desempeño de la labor policial operativa.

En este sentido, las Tecnologías de la Información y Comunicaciones aportan diferentes soluciones a las áreas de seguridad pública, tales como: proporcionar información cartográfica, estadística y documental; posicionamiento global determinado por satélite (GPS) para unidades móviles; cámaras de filmación con transmisión simultánea; base de datos con huellas dactilares digitalizadas, entre otras, que se pueden llegar a implementar.

Esas tecnologías proporcionan las herramientas eficientes y eficaces para poder prevenir, actuar y esclarecer delitos, apoyándose en equipos de última generación, con total conectividad y con los ciudadanos disponiendo efectivamente de la tecnología de conectividad total.

Asimismo, pueden consolidar la interoperabilidad de equipos de comunicación de las instituciones policiales a través de la sustitución de los equipos analógicos a digitales, y/o la integración de ambos en plataformas de última generación con una tendencia gradual hacia dispositivos que tengan la capacidad de transporte de datos, imágenes, videos y voz en tiempo real, permitiendo una facilidad de uso y mejora de la respuesta ciudadana y la integración de infraestructuras existentes.

En consecuencia, las Tecnologías de la Información y Comunicaciones, junto con el esfuerzo policiaco, son el basamento de los principales componentes que comprenden la seguridad pública y en parte de la seguridad nacional. De esta circunstancia puede deducirse que dichas tecnologías juegan un papel esencial en la prevención, lucha e investigación contra la criminalidad y en eso radica su extraordinaria importancia para la seguridad pública.

Por lo tanto, resulta indudables que los Complejos de Seguridad, junto con las bases de datos criminalísticas y toda la tecnología que la soporta, a nivel estatal y nacional, participan de la importancia que tienen dichas tecnologías, por ser el soporte fundamental de la operación de ambas. Consecuentemente, la pertinencia, suficiencia y calidad de esas tecnologías es un asunto también, de la mayor importancia.

Durante los años 2016 a 2017 el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, llevó a cabo un diagnóstico de los Complejos de Seguridad (C4 y C5), tanto para conocer la suficiencia del equipamiento tecnológico que lo soporta, como para determinar la variedad, en términos de calidad y pertinencia de los mismos, a lo largo de todo el territorio nacional. Posteriormente, se han realizado otros diagnósticos parciales o con distintos objetivos de los que se desprende la siguiente problemática.

La evolución de la adopción tecnológica y de la información, ha sido desorganizada y desarticulada a lo largo del país, dada la diversidad de sistemas, comunicaciones y servicios inconexos, lo que obedece a que la coordinación, comunicación, interoperabilidad e intercambio de información, entre gobiernos, es **discrecional y no obligatoria**.

Las bases de datos nacionales no tienen la utilidad deseable por ser relativamente cerradas, mientras que las estatales y locales, crecen y se reproducen en lenguajes, estructuras y formatos distintos, dando lugar a duplicidades de información — registro y captura—, con desaprovechamiento para fines de despliegue operativo, inteligencia policial y combate a la impunidad.

Al respecto, el marco jurídico reglamentario de la Constitución en la materia es insuficiente. Por un lado, la Ley General del Sistema Nacional de Seguridad Pública se enfoca fundamentalmente en establecer competencias y mecanismos de coordinación entre los tres órdenes de gobierno, sin que existan disposiciones sobre las tecnologías, su implementación, renovación, mantenimiento, uso, compatibilidad interoperación y aprovechamiento, lo que queda a discreción de los integrantes del sistema nacional, incluyendo a los gobiernos estatales y municipales, quienes han establecido reglas propias y no necesariamente convergentes para un sistema nacional.

En ese sentido, "...en la actualidad el federalismo debe cumplir ante todo dos funciones: la estructuración del poder por medio de la división vertical de poderes [...]..."

El problema de esta definición es que conduce a la adopción de un acercamiento al federalismo puramente técnico y a su reducción al estatus de una caja de herramientas. Sin embargo, mientras que el federalismo de hecho representa una caja de herramientas en cierto grado, es más que eso, dado que incorpora aspiraciones fundamentales. Desde un punto de vista legal, debemos mirar más allá de las provisiones constitucionales explícitas, con la intención de reflejar los valores que conducen a la creación de una federación y a los valores que el federalismo implica cuando una federación existe<sup>10</sup>.

El artículo 40 de la Constitución establece el carácter federal de la organización política mexicana y reconoce al federalismo como un arreglo institucional que se distingue por la división de poderes entre un gobierno federal y los gobiernos de los estados miembros.

El vínculo entre el federalismo y la diversidad puede provenir de dos perspectivas diferentes; la primera que procede de la creencia en el valor intrínseco de la misma y de la necesidad de perfilar consecuencias constitucionales de esa diversidad; la segunda que proviene del mero conocimiento de que la presencia de las comunidades políticas diversas en un mismo territorio es mejor dirigida con la creación de un sistema federal. Es una racionalidad verdaderamente importante, al resultar del reconocimiento de los derechos que tienen los grupos particulares, así como los arreglos institucionales<sup>11</sup>.

En México, en estas tendencias hacia un federalismo moderno, en tanto para asumir responsabilidades de una manera más eficiente y eficaz en los tres ámbitos de gobierno, se incentivaron prácticas de descentralización que se traducen en la "transferencia de facultades o atribuciones del Gobierno federal hacia otros órdenes de gobierno, teniendo como objetivos:

- La eficiencia administrativa y eficiencia en la organización política, administrativa y jurídica del Estado.
- El mejoramiento de la planificación de las tareas del Estado.
- Incremento en la eficiencia de la gestión y operación de los servicios públicos.
- Alcanzar una mayor equidad en el ejercicio del gasto público.
- Distribuir mejor los servicios del Estado hacia la población y lograr que el desarrollo sea equilibrado y equitativo para todas las regiones.
- Mejorar la participación política de la población en las decisiones públicas.

<sup>10</sup> [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S0041-86332006000300003](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332006000300003)

<sup>11</sup> <http://www.ordenjuridico.gob.mx/Congreso/CongresoInt/ponencias/JFGD.pdf>

Tales objetivos se presentan en la realidad de los tres ámbitos de gobierno como los grandes retos a ser superados y, en consecuencia, a ser incorporados en la vida política, económica, social y administrativa de la nación mexicana, con el fin de constituirse como una nueva cultura que, a su vez, se traduzca en una mejor forma de relacionamiento entre gobierno y ciudadanía<sup>12</sup>.

Por el otro lado, se encuentran disposiciones secundarias como son las normas técnicas establecidas por el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, cuyo propósito es estandarizar la tecnología empleada en Seguridad Pública con la finalidad de establecer parámetros técnicos que sirvan como referencia para la elaboración de proyectos nuevos de complejos de seguridad, o bien para mejorar los existentes, atendiendo con ello a la innecesaria heterogeneidad que priva y al objetivo de sentar las bases para la convergencia entre los sistemas y tecnologías de México en la materia.

Esas normas técnicas se formularon en primer término para los Centros de Atención de Llamadas de Emergencia (CALLES), en segundo término, para los Sistemas de Videovigilancia y, por último, la dedicada a los Complejos de Seguridad para homologar características, tecnología, infraestructura y sistemas de dichos Complejos. Esta última está en proceso de aprobación como una Norma Oficial Mexicana, conforme a la Ley Federal de Metrología y Normalización, con el fin de asegurar su aplicación y obligatoriedad en todo el territorio nacional.

Estos esfuerzos de estandarización técnica, si bien importantes, resultan parciales en sus alcances y limitados en su cumplimiento dado que los miembros del Sistema Nacional de Seguridad Pública en Estados y municipios, los aplican discrecionalmente y exclusivamente para proyectos financiados con recursos federales provenientes del FASP y FORTASEG, sin que resulten obligados en aquellos financiados con recursos de cualquier otro origen, propios, contratación de deuda o proyectos de prestación de servicios.

A las normas técnicas de estandarización del Sistema Nacional se suman una multiplicidad de disposiciones y requerimientos específicos establecidos para Estados y Municipios por distintas áreas del gobierno federal mediante los cuales solicitan e instruyen requerimientos de información, especificaciones, sistemas, equipos y requisitos técnicos aplicables para temas diversos como son la radiocomunicación, los registros nacionales en múltiples áreas de política pública, la operación de las bases de datos nacionales, la geolocalización, entre otros.

Así, los gobiernos estatales y municipales están sujetos a una serie de normas, lineamientos, requisitos y requerimientos provenientes de múltiples instancias federales, además de sus propias leyes y reglas establecidas en materia de información y tecnologías para la seguridad pública, que operan simultáneamente

---

<sup>12</sup> [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S1405-14352009000100009](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-14352009000100009)

sin que necesariamente sus esfuerzos sean coordinados, convergentes y compatibles.

En particular, en materia de información y comunicaciones existen áreas sustantivas del gobierno federal con funciones y atribuciones superpuestas que no contribuyen generar el ambiente de certeza y eficacia necesario para los gobiernos estatales y municipales. Tal es el caso del Centro Nacional de Información del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y del Centro Nacional de Información Plataforma México, ambas áreas integrantes de la Secretaría de Seguridad y Protección Ciudadana.

Esta duplicidad quizá justificada en el nacimiento de ambas áreas en Secretarías de Estado distintas en el sexenio 2006-2012, es hoy innecesaria e ineficiente para la operación y buen desempeño de las instituciones encargadas de la seguridad en todo el país.

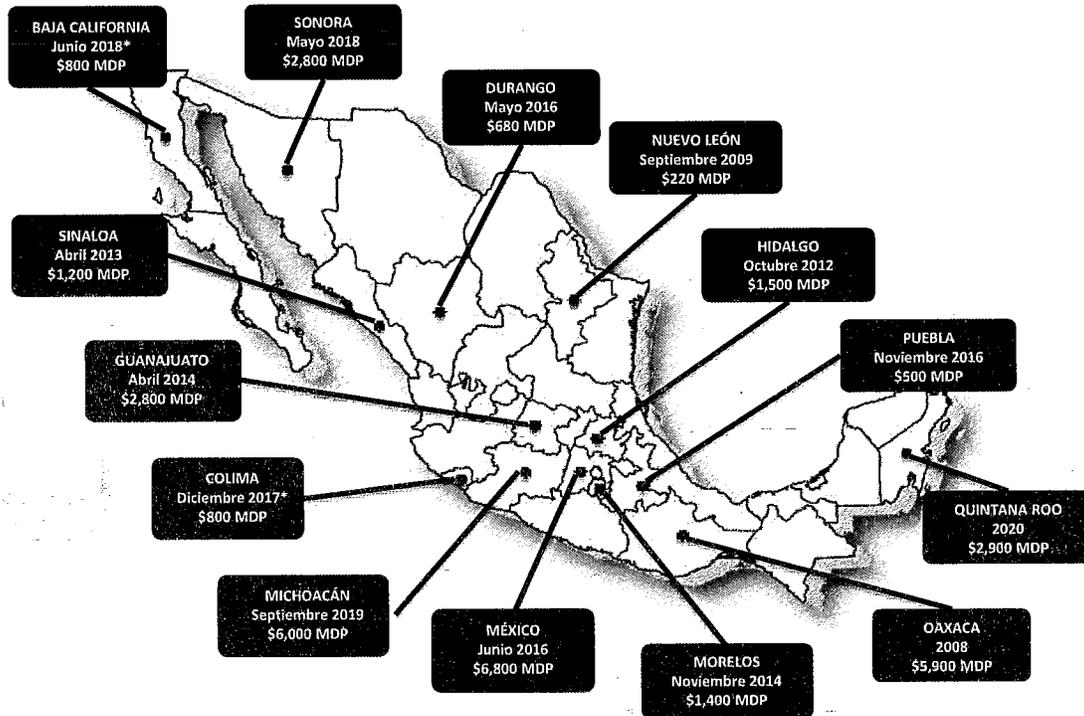
En este contexto, subsisten duplicidad de requerimientos, multiplicidad de disposiciones normativas y asimetrías en la información y las especificaciones sobre los servicios y bases técnicas que la infraestructura y tecnologías de las comunicaciones deben establecerse, ocasionando que los gobiernos carezcan de certidumbre sobre la pertinencia, viabilidad y eficiencia de lo que adquieren, generándose costos excesivos y gastos innecesarios que dificultan la operación y encarecen innecesariamente los proyectos de infraestructura.

La disparidad y problemática en la evolución de las tecnologías de información y telecomunicaciones de seguridad pública se observa claramente en los Centros de Control, Comando, Cómputo y Comunicaciones, conocidos como C4s. Estos Centros constituyen complejos en los que se integran y operan los sistemas y demás herramientas tecnológicas de apoyo a la seguridad pública. En México existe al menos un Centro por entidad federativa y, bajo distintas arquitecturas dependiendo de la entidad federativa, más de 60 subcentros.

En años recientes, los Centros han sido los principales proyectos tecnológicos en materia de seguridad. De manera creciente las inversiones se destinan a estos proyectos que han dado lugar a una competencia entre los gobiernos de los estados por construir Centros más grandes y costosos, en el ánimo de contar con más y mejor tecnología, llegando a aumentar el número de "C" en el acrónimo para referir diversos atributos o servicios añadidos a las cuatro "C" originales. Partiendo de 2009 cuando se instaló el primer C4, en la CDMX, se tuvo primero la instalación de un C4 en cada estado. Para 2017 había 8 Centros estatales autodenominados C5. En 2020 se tienen al menos 14 Centros estatales autodenominados C5 e incluso el primer C6 en el Estado de Hidalgo.

Por su naturaleza, dimensiones y complejidad los Centros suponen costos elevados y destacan como el principal destino de gasto público en seguridad. Se estima que su creación ha costado al país en total alrededor de \$50 ml millones de pesos en los últimos 10 años. En ese sentido, transformar las reglas para mejorar su diseño e implementación, racionalizar sus costos y favorecer su mantenimiento, operación

y actualización tendrá un impacto favorable en la asignación y uso de los recursos públicos en seguridad.



En efecto, la ausencia de un marco normativo único, de estándares técnicos obligatorios y de reglas que permitan valorar su necesidad y características así como de procedimientos para verificar y certificar los Centros hacen hoy muy difícil conocer sus especificaciones, desempeño, aprovechamiento y resultados, favoreciendo la ineficacia y el dispendio de recursos, además de dificultar la construcción de una red nacional de centros que permita interoperar en beneficio de la seguridad en todo el país, privilegiando la inteligencia.

Así, los vacíos del marco normativo vigente, la persistencia de duplicidades administrativas y la aplicación parcial y discrecional de los estándares técnicos disponibles han contribuido a generar un contexto propicio para el crecimiento desarticulado de la infraestructura tecnológica para información y comunicaciones, así como para el dispendio y la ineficiencia en el uso de los recursos públicos.

Se requiere solventar estas insuficiencias de un marco legal específico, mediante una Ley que resuelva la indefinición de principios rectores, sujetos obligados, responsabilidades, atribuciones y criterios técnicos, entre otros, que terminen con la incertidumbre y discrecionalidad, efectivamente contribuyendo a eliminar espacios para posibles prácticas de corrupción y a sentar las bases para el desarrollo

ordenado de las tecnologías de la información y las comunicaciones a nivel nacional.

Por último, es necesario armonizar las disposiciones en materia de información y comunicación con la evolución misma de las instancias de seguridad pública y procuración de justicia, así como la delimitación de responsabilidades y atribuciones en la generación de información. En este sentido, las disposiciones orientadas a la estandarización e interoperabilidad de las tecnologías, así como para la generación y gestión de información y bases de datos a nivel nacional requiere de normar tanto a las instituciones de procuración de justicia, hoy Fiscalías autónomas, así como armonizarse con los usos y necesidades de la recientemente creada Guardia Nacional.

En consecuencia, de todo lo expuesto, se ha concluido en la necesidad de crear una Ley Nacional de aplicación en todo el país que no sólo regule al Sistema Nacional de Información en Seguridad Pública, como lo establece el Artículo 21, párrafo 10 de la Constitución<sup>13</sup>, sino que además comprenda las bases técnicas para la estandarización de las tecnologías de la información y comunicaciones requeridas por la seguridad pública.

Crear una Ley Nacional es el instrumento idóneo para regular el ordenamiento, uso, desarrollo e interconexión de las tecnologías para la seguridad pública en México, lo que no se lograría con reformas a las leyes existentes. La ley propuesta atiende el problema de fondo en aspectos clave, como reforzar y privilegiar la inteligencia, misma que está orientada a conocer con profundidad todos los aspectos relacionados con los fenómenos que representan amenazas y riesgos a la seguridad nacional; como lo son las posibles manifestaciones de los mismos, su probabilidad de ocurrencia e impacto, las variables que los componen y la relación causal entre las mismas. Uno de los principales rasgos de la inteligencia es la confidencialidad, lo que permite evitar que la capacidad del Estado para poner en marcha medidas en la materia sea neutralizada.

Una Ley Nacional es de cumplimiento obligatorio en todo el país, cerrando el paso a prácticas, normas y discrecionalidad por parte de Estados y municipios, toda vez que la Ley General del Sistema Nacional de Seguridad Pública actual, establece competencias y mecanismos de coordinación entre los tres órdenes de gobierno, dejando a Estados y municipios la posibilidad de establecer sus propias reglas sobre las tecnologías y su aprovechamiento.

La Ley propuesta, permite crear y normar un Sistema Nacional sobre la información y las comunicaciones de seguridad pública de manera integral, estableciendo ordenamientos obligatorios a todos los actores institucionales relevantes que participan de la generación, administración y aprovechamiento de las tecnologías de la información y las comunicaciones, incluyendo a la Guardia Nacional y los órganos autónomos.

---

<sup>13</sup> [http://www.diputados.gob.mx/LeyesBiblio/pdf/1\\_080520.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf)

Ello permitirá además subsanar deficiencias del marco legal actual estableciendo definiciones, criterios y disposiciones sobre temas cruciales como son: infraestructuras críticas, telecomunicaciones, complejos de seguridad, entre otros, establecer normas y estándares específicos en todas las áreas de los sistemas, tecnologías e infraestructuras críticas. Adicionalmente será el instrumento idóneo para establecer reglas, criterios y obligaciones que aseguren una adecuada contratación e implementación.

Asimismo, dicha Ley permite regular a las Fiscalías autónomas, precisando sus atribuciones y responsabilidades en materia de información y el uso de tecnologías. Así también establecerá los límites para dirimir diferencias que se tienen en cuanto a la generación y manejo de la información entre los poderes ejecutivos federal y estatales y organismos especializados como el INEGI, por ejemplo, dejar en claro los alcances y tramos de responsabilidad en materia de generación de inventarios de personal o bien de la generación y publicación de datos, información y estadísticas criminales.

La propuesta de Ley armoniza el uso de tecnologías con la Guardia Nacional, que tiene obligaciones y atribuciones que dependen de su acceso a tecnologías (DOF 27-05-2019)<sup>14</sup>. Es deseable establecer el marco normativo que precise su participación y niveles de acceso. Actualmente, los Complejos de Seguridad son propiedad y monopolio de los gobiernos estatales y locales. La comunicación y colaboración entre corporaciones depende más de la voluntad que del marco normativo.

El marco legal integral que se propone permitirá normar temas nuevos, de vanguardia, que se integrarán a las normas aplicables a los servicios tradicionales que regulan los Complejos de Seguridad. Entre éstos se encuentran: criterios generales para la contratación, administración, diseño, desarrollo, implementación, operación, mantenimiento y sustentabilidad de los Complejos de Seguridad; sistema de precios de referencia, padrón de proveedores y convenios marco, como instrumentos que permitan establecer condiciones de competencia equitativa en el mercado, evitando asimetrías de información que permiten ineficiencias y corrupción; instancias para la evaluación, auditoría técnica y certificación de los Complejos de Seguridad como mecanismos para el aseguramiento de la calidad y los estándares establecidos; bases para la integración de la Red Nacional de Complejos de Seguridad; y obligaciones de colaboración de particulares e interoperabilidad de sistemas privados para fines de seguridad pública.

Por último, es de la mayor importancia la creación de una instancia que proporcione certidumbre, eficacia y racionalidad técnica, tanto a la regulación que prescribe la Ley que se propone, como a la conducción, ejecución, instrumentación y evaluación de las acciones que la misma implican, y que considerando las actuales normas de austeridad se concrete con la fusión y unificación de los actuales: Centro Nacional

---

<sup>14</sup> [https://www.dof.gob.mx/nota\\_detalle.php?codigo=5561285&fecha=27/05/2019](https://www.dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019)

de Información y la Plataforma México, que a nivel nacional tienen un mínimo de coordinación y en el contexto de la Nación como un todo permitan eliminar la discrecionalidad de las entidades federativas y los municipios.

El proyecto legislativo de la **“LEY NACIONAL DEL SISTEMA NACIONAL DE LA INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD PÚBLICA”** que ahora se presenta, se divide en: seis títulos, veinticinco capítulos y diecinueve secciones. Se inspira en una serie de principios rectores que deben servir de fundamento de la política del Estado en materia de tecnologías de la información y las comunicaciones en seguridad pública.

Entre esos principios destacan la salvaguarda del bien jurídico tutelado que es la vida; la atención de las emergencias con un enfoque integral, la video vigilancia incluyendo el apoyo de los particulares y los servicios para la atención de las llamadas de denuncia anónima como servicios con filosofía asistencial, particularmente para las personas que emiten las llamadas generalmente en estado crítico; la equidad entre nacionales y extranjeros; y la independencia de los servicios de atención de las llamadas de emergencia, de los de prestación material de los auxilios.

El Título Primero de “Disposiciones Preliminares” señala el objeto, premisas fundamentales y definiciones de la ley.

El Título Segundo “De la Distribución de Competencias”, consta de tres capítulos. En el capítulo primero se establecen las de la Federación. En el capítulo segundo las competencias de las Entidades Federativas y en capítulo tercero las competencias de los municipios.

El Título Tercero “Del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública”, consta de nueve capítulos. En el capítulo primero, se establece la finalidad, objetivo, naturaleza y principios del Sistema. En el capítulo segundo, se señala los componentes básicos del Sistema. En el capítulo tercero y cuarto la organización y la estructura funcional del Sistema, respectivamente.

En el capítulo quinto de este título, el Subsistema de Recopilación y Almacenamiento de Datos e Información. En el capítulo sexto el Subsistema de Procesamiento e Integración de las Bases de Datos. En el séptimo, el Subsistema de Explotación, Uso y Diseminación de la Información; en el octavo, el Subsistema de Interoperabilidad y Comunicaciones, finalmente el capítulo noveno las Disposiciones Reguladoras de los Concesionarios de Telecomunicación y de los Prestadores de Servicio de Auxilio.

El Título Cuarto “Del Instituto Nacional del Sistema de la Información y Comunicaciones para la Seguridad Pública”, consta de seis capítulos. En el primero, de las disposiciones generales se fijan las bases para la creación de ese Instituto Nacional.

En su segundo capítulo de este título, de su organización y funcionamiento, se establecen las funciones y administración, señalando que esta última estará en manos de una Junta de Gobierno y un Director General, con las atribuciones de unos y otro.

En el tercer capítulo, se establecen la organización y funcionamiento de las Unidades Administrativas del Instituto. En el cuarto capítulo, del Patrimonio del Instituto, se establece la integración de su patrimonio, así como el presupuesto para su operación.

En el capítulo quinto de este título, de la información, se establece la confidencialidad de los datos proporcionados por los usuarios del Sistema, la transmisión de la información y de la compatibilidad de la misma. En el capítulo sexto, de la profesionalización del personal del Instituto, se establece la forma y requisitos para su ingreso y permanencia.

El Título Quinto “De las Tecnologías de la Información y Comunicaciones”, consta de cinco capítulos. En el capítulo primero, la Formulación de Proyectos de Infraestructura Física, de Información y de Comunicaciones; se establecen las reglas generales para la formulación de proyectos generales y ejecutivos, los indicadores para su programación y evaluación, la seguridad de la información y de la considerada de seguridad nacional. –

En el capítulo segundo de este título, del Equipamiento (Hardware) de TIC, se establece la infraestructura de tecnología de información mínima central, regional y de los Complejos de Seguridad; así como de las redes de comunicación locales, estatales y Nacional. En el capítulo tercero, los Programas Informáticos (Software) para las Facilidades Funcionales de TIC, se establece lo referente al Sistema de Gestión de Incidentes (CAD) y a la Red LAN. En el capítulo cuarto, de los Procesos de Adquisición, se fijan las disposiciones a las que deberá sujetarse la contratación de TIC. Finalmente, en el capítulo cinco de los procesos de funcionamiento de TIC, se dispone lo relacionado a la implementación, operación, conservación y mantenimiento de TIC.

En el Título Sexto “De las Faltas Administrativas de los Usuarios y de las Responsabilidades de los Servidores Públicos”. Este título consta de dos capítulos. En el primero, de las faltas administrativas y de los delitos, cometidos, tanto por servidores públicos como por personas ajenas al servicio público. Finalmente, en su capítulo segundo, se establecen las responsabilidades para los servidores que las cometen, señalando las sanciones a que se hacen acreedores. Finalmente, los ARTÍCULOS TRANSITORIOS.

En resumen, en el convencimiento de que el bien jurídico tutelado por la Ley, que es la vida, es de importancia capital en el desarrollo de la sociedad, por ser la base de ésta, es de considerarse que el proyecto de la “**LEY NACIONAL DEL SISTEMA NACIONAL DE LA INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD PÚBLICA**” no sólo apoyará a las tecnologías de la información y comunicaciones, sino que permitirá además uniformar y homogenizar los servicios

de los Complejos de Seguridad en todo el territorio nacional, en beneficio de la sociedad y por ende de la nación.

**Derivado de lo anterior, en esta iniciativa propone la siguiente modificación:**

**Ley General del Sistema Nacional de Seguridad Pública.**

TEXTO VIGENTE	TEXTO PROPUESTO
<p>Artículo 5 ...</p> <p>I. ...</p> <p>II. ...</p> <p>III. ...</p> <p>IV. ...</p> <p>V. ...</p> <p>VI. Conferencias Nacionales: a las Conferencias a las que se refiere el artículo 10 de esta Ley;</p> <p>VII. Consejo Nacional: al Consejo Nacional de Seguridad Pública;</p> <p>VIII. Instituciones de Seguridad Pública: a las Instituciones Policiales, de Procuración de Justicia, del Sistema Penitenciario y dependencias encargadas de la Seguridad Pública a nivel federal, local y municipal;</p> <p>IX. Instituciones de Procuración de Justicia: a las Instituciones de la Federación y entidades federativas que integran al Ministerio Público, los servicios periciales, policías de investigación y demás auxiliares de aquel;</p>	<p>Artículo 5 ...</p> <p>I. ...</p> <p>II. ...</p> <p>III. ...</p> <p>IV. ...</p> <p>V. ...</p> <p><b>VI. Centro Nacional de Información: al Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública.</b></p> <p>VII. Conferencias Nacionales: a las Conferencias a las que se refiere el artículo 10 de esta Ley;</p> <p>VIII. Consejo Nacional: al Consejo Nacional de Seguridad Pública;</p> <p>IX. Instituciones de Seguridad Pública: a las Instituciones Policiales, de Procuración de Justicia, del Sistema Penitenciario y dependencias encargadas de la Seguridad Pública a nivel federal, local y municipal;</p>

<p>X. Instituciones Policiales: a los cuerpos de policía, de vigilancia y custodia de los establecimientos penitenciarios, de detención preventiva, o de centros de arraigos; y en general, todas las dependencias encargadas de la seguridad pública a nivel federal, local y municipal, que realicen funciones similares;</p>	<p>X. Instituciones de Procuración de Justicia: a las Instituciones de la Federación y entidades federativas que integran al Ministerio Público, los servicios periciales, policías de investigación y demás auxiliares de aquel;</p>
<p>XI. Institutos: a los órganos de las instituciones de seguridad pública de la Federación, de los Estados y del Distrito Federal, encargados de la formación y actualización especializada de aspirantes y servidores públicos de las funciones ministerial, pericial y de policía ministerial;</p>	<p>XI. Instituciones Policiales: a los cuerpos de policía, de vigilancia y custodia de los establecimientos penitenciarios, de detención preventiva, o de centros de arraigos; y en general, todas las dependencias encargadas de la seguridad pública a nivel federal, local y municipal, que realicen funciones similares;</p>
<p>XII. Programa Rector: al conjunto de contenidos encaminados a la profesionalización de los servidores públicos de las Instituciones Policiales e Instituciones de Procuración de Justicia, respectivamente;</p>	<p>XII. Institutos: a los órganos de las instituciones de seguridad pública de la Federación, de los Estados y del Distrito Federal, encargados de la formación y actualización especializada de aspirantes y servidores públicos de las funciones ministerial, pericial y de policía ministerial;</p>
<p>XIII. Registro Nacional: el Registro Nacional de Personal de las Instituciones de Seguridad Pública;</p>	<p>XIII. Programa Rector: al conjunto de contenidos encaminados a la profesionalización de los servidores públicos de las Instituciones Policiales e Instituciones de Procuración de Justicia, respectivamente;</p>
<p>XIV. Secretaría: a la Secretaría de Seguridad y Protección Ciudadana del Gobierno Federal;</p>	<p>XIV. Registro Nacional: el Registro Nacional de Personal de las Instituciones de Seguridad Pública;</p>
<p>XV. Secretario Ejecutivo: el Titular del Secretariado Ejecutivo del Sistema;</p>	<p>XV. Secretaría: a la Secretaría de Seguridad y Protección Ciudadana del Gobierno Federal;</p>

<p>XVI. Sistema: al Sistema Nacional de Seguridad Pública, y</p> <p>XVII. Sistema Nacional de Información: al Sistema Nacional de Información en Seguridad Pública, el cual constituye el conjunto integrado, organizado y sistematizado de las Bases de Datos. Está integrado por elementos metodológicos y procedimentales que permiten a las Instituciones de Seguridad Pública su consulta e interconexión para el desempeño de sus funciones.</p> <p>Artículo 17.- El Secretariado Ejecutivo es el órgano operativo del Sistema y gozará de autonomía técnica, de gestión y presupuestal. Contará con los Centros Nacionales de Información, de Prevención del Delito y Participación Ciudadana, así como de Certificación y Acreditación. El Titular del Ejecutivo Federal expedirá el Reglamento del Secretariado, que establecerá las atribuciones y articulación de estos Centros.</p> <p>...</p> <p>I ...</p> <p>II ...</p> <p>III ...</p> <p>IV ...</p> <p>V ...</p>	<p><b>XVI.</b> Secretario Ejecutivo: el Titular del Secretariado Ejecutivo del Sistema;</p> <p><b>XVII.</b> Sistema: al Sistema Nacional de Seguridad Pública, y</p> <p><b>XVIII.</b> Sistema Nacional de Información: al Sistema Nacional de <b>la Información y Comunicaciones para la Seguridad Pública, a que se refiere la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública.</b></p> <p><b>Artículo 17.-</b> El Secretariado Ejecutivo es el órgano operativo del Sistema y gozará de autonomía técnica, de gestión y presupuestal. Contará con los <b>Centros Nacionales de Prevención del Delito y Participación Ciudadana</b>, así como de Certificación y Acreditación. El Titular del Ejecutivo Federal expedirá el Reglamento del Secretariado, que establecerá las atribuciones y articulación de estos Centros.</p> <p>...</p> <p>I ...</p> <p>II ...</p> <p>III ...</p> <p>IV ...</p> <p>V ...</p>
---	--

~~Artículo 19.~~ El Centro Nacional de Información será el responsable de regular el Sistema Nacional de Información y tendrá, entre otras, las siguientes atribuciones:

~~I.~~ Determinar los criterios técnicos y de homologación de las Bases de Datos que conforman el Sistema Nacional de Información;

~~II.~~ Emitir los lineamientos de uso, manejo y niveles de acceso al Sistema Nacional de Información;

~~III.~~ Conocer, integrar y analizar las Bases de Datos del Sistema Nacional de Información, en términos de los lineamientos que al efecto emita;

~~IV.~~ Vigilar el cumplimiento de los criterios de acceso a la información y hacer del conocimiento de las instancias competentes cualquier irregularidad detectada;

~~V.~~ Colaborar con el Instituto Nacional de Estadística y Geografía, así como celebrar convenios con ese organismo para la integración de la estadística nacional en materia de seguridad pública, de conformidad con la ley y los lineamientos que emita el Sistema Nacional, y

~~VI.~~ Brindar asesoría a las Instituciones de Seguridad Pública para la integración y uso de la información de las Bases de Datos al Sistema Nacional de Información.

TÍTULO SÉPTIMO DEL SISTEMA NACIONAL DE INFORMACIÓN EN SEGURIDAD PÚBLICA

**Artículo 19.- Derogado.**

TÍTULO SÉPTIMO  
DEL SISTEMA NACIONAL DE LA  
INFORMACIÓN  
Y

<p>Artículo 109 Bis. - <del>La Secretaría</del> será la encargada de la operación de la plataforma tecnológica que sustenta el Sistema Nacional de Información, a través de la unidad administrativa que su titular determine. Dicha unidad tendrá, entre otras, las siguientes atribuciones:</p> <p>I. ...  II. ...  III. ...  IV. ...</p> <p>V. Proponer, <del>en coordinación con el Centro Nacional de Información,</del> el Plan Anual de Desarrollo y Modernización Tecnológica al Consejo Nacional de Seguridad Pública;</p> <p>VI. ...  VII. ...  VIII. ...</p>	<p><b>COMUNICACIONES PARA LA SEGURIDAD PÚBLICA</b></p> <p><b>Artículo 109 Bis. - El Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública</b> será la encargada de la operación de la plataforma tecnológica que sustenta el Sistema Nacional de Información, a través de la unidad administrativa que su titular determine. Dicha unidad tendrá, entre otras, las siguientes atribuciones:</p> <p>I. ...  II. ...  III. ...  IV. ...</p> <p>V. Proponer <b>el Plan Anual de Desarrollo</b> y Modernización Tecnológica al Consejo Nacional de Seguridad Pública;</p> <p>VI. ...  VII. ...  VIII. ...</p>
---	--

**Ley del Sistema Nacional de Información Estadística y Geográfica.**

TEXTO VIGENTE	TEXTO PROPUESTO
<p>ARTÍCULO 33.- ...</p> <p>I a la VII ...</p> <p>...  ...  ...</p>	<p>ARTÍCULO 33.- ...</p> <p>I a la VII ...</p> <p>...  ...  ...</p>

<p><b>SIN CORRELATIVO</b></p>	<p><b>El Instituto Nacional de la Información y Comunicaciones para la Seguridad Pública determinará las normas relativas a la información que produzca y requiera, en materia de seguridad pública, sin menoscabo de participar en los comités: ejecutivo y técnico especializado, que corresponda para la debida coordinación con el INEGI.</b></p>
-------------------------------	---

**Ley de la Guardia Nacional.**

<p><b>TEXTO VIGENTE</b></p>	<p><b>TEXTO PROPUESTO</b></p>
<p>Artículo 9. ...</p> <p>I a la XXIII...</p> <p>XXIV. Incorporar a las Bases de Datos del Sistema Nacional de Información en Seguridad Pública la información que pueda ser útil en la investigación de los delitos y utilizar su contenido para el desempeño de sus atribuciones, sin afectar el derecho de las personas a la protección de sus datos personales;</p> <p>XXV a XXXIX. ...</p> <p>XL. Integrar al Sistema Nacional de Información en Seguridad Pública los datos que se recaben para identificar a las personas;</p>	<p>Artículo 9. ...</p> <p>I a la XXIII...</p> <p><b>XXIV.</b> Incorporar a las Bases de Datos del Sistema Nacional de la Información <b>y Comunicaciones para la Seguridad Pública, con estricto apego a las normas establecidas al efecto por el Instituto Nacional del Sistema de Información y Comunicaciones para la Seguridad Pública</b> la información que pueda ser útil en la investigación de los delitos y utilizar su contenido para el desempeño de sus atribuciones, sin afectar el derecho de las personas a la protección de sus datos personales;</p> <p>XXV a XXXIX. ...</p> <p><b>XL.</b> Integrar al Sistema Nacional de la Información <b>y Comunicaciones para la Seguridad Pública con estricto apego a las normas establecidas al efecto por el Instituto Nacional del Sistema de Información y Comunicaciones para la Seguridad</b></p>

XLI a la XLIV. ...	<b>Pública</b> los datos que se recaben para identificar a las personas;  XLI a la XLIV. ...
--------------------	--

**Ley Orgánica de la Fiscalía General de la República.**

<b>TEXTO VIGENTE</b>	<b>TEXTO PROPUESTO</b>
<p>Artículo 26. ...</p> <p>I a la VIII. ...</p> <p>a. El intercambio de información, documentación, bases de datos, a través de sistemas de interoperabilidad;</p> <p>b. ...</p> <p>c. ...</p> <p>d. ...</p> <p>e. ...</p> <p>f. ...</p> <p>IX a la X. ...</p>	<p>Artículo 26. ...</p> <p>I a la VIII. ...</p> <p>a. El intercambio de información, documentación, bases de datos, a través de sistemas de interoperabilidad, <b>particularmente con el Instituto Nacional del Sistema de la Información y Comunicaciones para la Seguridad Pública respecto de la información que en su caso puedan requerir las bases de datos nacionales del Sistema Nacional de Seguridad Pública, así como las necesarias para la integración de las estadísticas de incidencia delictiva del orden federal;</b></p> <p>b. ...</p> <p>c. ...</p> <p>d. ...</p> <p>e. ...</p> <p>f. ...</p> <p>IX a la X. ...</p>

**Ley Federal de Telecomunicaciones y Radiodifusión.**

TEXTO VIGENTE	TEXTO PROPUESTO
<p>Artículo 3. ...</p> <p>I. a la XXVII. ...</p> <p>XXVIII. Instituto: Instituto Federal de Telecomunicaciones;</p> <p>XXIX. Insumos esenciales: Elementos de red o servicios que se proporcionan por un solo concesionario o un reducido número de concesionarios, cuya reproducción no es viable desde un punto de vista técnico, legal o económico y son insumos indispensables para la prestación de los servicios de telecomunicaciones y de radiodifusión. En los casos no previstos en esta Ley, el Instituto determinará la existencia y regulación al acceso de insumos esenciales en términos de lo dispuesto por la Ley Federal de Competencia Económica;</p>	<p>Artículo 3. ...</p> <p>I. a la XXVII. ...</p> <p><b>XXVIII.- Instancias de Seguridad o Instancias de Seguridad y Procuración de Justicia. - Comprende a las Instituciones de Seguridad Pública a que se refiere la fracción VIII del artículo 5 de Ley General del Sistema Nacional de Seguridad Pública y al Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública de la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;</b></p> <p>XXIX. Instituto: Instituto Federal de Telecomunicaciones;</p>

**XXX.** Interconexión: Conexión física o virtual, lógica y funcional entre redes públicas de telecomunicaciones que permite la conducción de tráfico entre dichas redes y/o entre servicios de telecomunicaciones prestados a través de las mismas, de manera que los usuarios de una de las redes públicas de telecomunicaciones puedan conectarse e intercambiar tráfico con los usuarios de otra red pública de telecomunicaciones y viceversa, o bien permite a los usuarios de una red pública de telecomunicaciones la utilización de servicios de telecomunicaciones provistos por o a través de otra red pública de telecomunicaciones;

**XXXI.** Interferencia perjudicial: Efecto de una energía no deseada debida a una o varias emisiones, radiaciones, inducciones o sus combinaciones sobre la recepción en un sistema de telecomunicaciones o radiodifusión, que puede manifestarse como degradación de la calidad, falseamiento o pérdida de información, que compromete, interrumpe repetidamente o impide el funcionamiento de cualquier servicio de radiocomunicación;

**XXXII.** Internet: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los

**XXX.** Insumos esenciales: Elementos de red o servicios que se proporcionan por un solo concesionario o un reducido número de concesionarios, cuya reproducción no es viable desde un punto de vista técnico, legal o económico y son insumos indispensables para la prestación de los servicios de telecomunicaciones y de radiodifusión. En los casos no previstos en esta Ley, el Instituto determinará la existencia y regulación al acceso de insumos esenciales en términos de lo dispuesto por la Ley Federal de Competencia Económica;

**XXXI.** Interconexión: Conexión física o virtual, lógica y funcional entre redes públicas de telecomunicaciones que permite la conducción de tráfico entre dichas redes y/o entre servicios de telecomunicaciones prestados a través de las mismas, de manera que los usuarios de una de las redes públicas de telecomunicaciones puedan conectarse e intercambiar tráfico con los usuarios de otra red pública de telecomunicaciones y viceversa, o bien permite a los usuarios de una red pública de telecomunicaciones la utilización de servicios de telecomunicaciones provistos por o a través de otra red pública de telecomunicaciones;

**XXXII.** Interferencia perjudicial: Efecto de una energía no deseada debida a una o varias emisiones, radiaciones, inducciones o sus combinaciones sobre la recepción en un sistema de telecomunicaciones o radiodifusión, que puede manifestarse como degradación de la calidad, falseamiento o pérdida de información, que

<p>paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única;</p>	<p>compromete, interrumpe repetidamente o impide el funcionamiento de cualquier servicio de radiocomunicación;</p>
<p><b>XXXIII.</b> Interoperabilidad: Características técnicas de las redes públicas, sistemas y equipos de telecomunicaciones integrados a éstas que permiten la interconexión efectiva, por medio de las cuales se asegura la provisión de un servicio de telecomunicaciones específico de una manera consistente y predecible; en términos de la entrega funcional de servicios entre redes;</p>	<p><b>XXXIII.</b> Internet: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única;</p>
<p><b>XXXIV.</b> Ley: Ley Federal de Telecomunicaciones y Radiodifusión;</p>	<p><b>XXXIV.</b> Interoperabilidad: Características técnicas de las redes públicas, sistemas y equipos de telecomunicaciones integrados a éstas que permiten la interconexión efectiva, por medio de las cuales se asegura la provisión de un servicio de telecomunicaciones específico de una manera consistente y predecible, en términos de la entrega funcional de servicios entre redes;</p>
<p><b>XXXV.</b> Localización geográfica en tiempo real: Es la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada;</p>	<p><b>XXXV.</b> Ley: Ley Federal de Telecomunicaciones y Radiodifusión;</p>
<p><b>XXXVI.</b> Mensaje Comercial: Mención dirigida al público o a un segmento del mismo durante corte programático, con el propósito de informar sobre la</p>	<p><b>XXXVI.</b> Localización geográfica en tiempo real: Es la ubicación aproximada en el momento en que se procesa una</p>

<p>existencia o características de un producto, servicio o actividad para inducir su comercialización y venta, en las estaciones de radiodifusión con concesión comercial y canales de televisión y audio restringidos. El mensaje comercial no incluye los promocionales propios de la estación o canal, ni las transmisiones correspondientes a los tiempos del Estado, y otros a disposición del Poder Ejecutivo, ni programas de oferta de productos y servicios;</p>	<p>búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada;</p>
<p><b>XXXVII.</b> Multiprogramación: Distribución de más de un canal de programación en el mismo canal de transmisión;</p>	<p><b>XXXVII.</b> Mensaje Comercial: Mención dirigida al público o a un segmento del mismo durante corte programático, con el propósito de informar sobre la existencia o características de un producto, servicio o actividad para inducir su comercialización y venta, en las estaciones de radiodifusión con concesión comercial y canales de televisión y audio restringidos. El mensaje comercial no incluye los promocionales propios de la estación o canal, ni las transmisiones correspondientes a los tiempos del Estado, y otros a disposición del Poder Ejecutivo, ni programas de oferta de productos y servicios;</p>
<p><b>XXXVIII.</b> Neutralidad a la competencia: Obligación del Estado de no generar distorsiones al mercado como consecuencia de la propiedad pública;</p>	<p><b>XXXVIII.</b> Multiprogramación: Distribución de más de un canal de programación en el mismo canal de transmisión;</p>
<p><b>XXXIX.</b> Órbita satelital: Trayectoria que recorre una estación espacial alrededor de la Tierra;</p>	<p><b>XXXIX.</b> Neutralidad a la competencia: Obligación del Estado de no generar distorsiones al mercado como consecuencia de la propiedad pública;</p>
<p><b>XL.</b> Patrocinio: El pago en efectivo o en especie que realiza cualquier persona</p>	

<p>física o moral a fin de que se haga la mención o presentación visual de la denominación, razón social, marca o logotipo de la persona que realizó el pago;</p> <p><b>XLII.</b> Películas cinematográficas: Creación audiovisual compuesta por imágenes en movimiento, con o sin sonorización incorporada, con una duración de sesenta minutos o superior. Son películas nacionales las realizadas por personas físicas o morales mexicanas o las realizadas en el marco de los acuerdos internacionales o los convenios de coproducción suscritos por el gobierno mexicano, con otros países u organismos internacionales;</p> <p><b>XLIII.</b> Poder de mando: La capacidad de hecho de influir de manera decisiva en los acuerdos adoptados en las asambleas de accionistas o sesiones del consejo de administración o en la gestión, conducción y ejecución de los negocios de una persona que ésta controle o en las que tenga una influencia significativa;</p> <p><b>XLIV.</b> Política de inclusión digital universal: Conjunto de programas y estrategias emitidos por el Ejecutivo Federal orientadas a brindar acceso a las tecnologías de la información y la comunicación, incluyendo el Internet de banda ancha para toda la población, haciendo especial énfasis en sus sectores más vulnerables, con el propósito de cerrar la brecha digital existente entre individuos, hogares, empresas y áreas geográficas de distinto nivel socioeconómico, respecto a sus oportunidades de acceso a las</p>	<p><b>XL.</b> Órbita satelital: Trayectoria que recorre una estación espacial alrededor de la Tierra;</p> <p><b>XLI.</b> Patrocinio: El pago en efectivo o en especie que realiza cualquier persona física o moral a fin de que se haga la mención o presentación visual de la denominación, razón social, marca o logotipo de la persona que realizó el pago;</p> <p><b>XLII.</b> Películas cinematográficas: Creación audiovisual compuesta por imágenes en movimiento, con o sin sonorización incorporada, con una duración de sesenta minutos o superior. Son películas nacionales las realizadas por personas físicas o morales mexicanas o las realizadas en el marco de los acuerdos internacionales o los convenios de coproducción suscritos por el gobierno mexicano, con otros países u organismos internacionales;</p> <p><b>XLIII.</b> Poder de mando: La capacidad de hecho de influir de manera decisiva en los acuerdos adoptados en las asambleas de accionistas o sesiones del consejo de administración o en la gestión, conducción y ejecución de los negocios de una persona que ésta controle o en las que tenga una influencia significativa;</p>
--	--

<p>tecnologías referidas y el uso que hacen de éstas;</p> <p>XLIV. Portabilidad: Derecho de los usuarios de conservar el mismo número telefónico al cambiarse de concesionario o prestador de servicio;</p> <p>XLV. Posiciones orbitales geoestacionarias: Ubicaciones en una órbita circular que se encuentran en el plano ecuatorial, que permiten que un satélite mantenga un periodo de traslación igual al periodo de rotación de la Tierra;</p> <p>XLVI. Preponderancia: Calidad determinada por el Instituto de un agente económico en los términos del artículo 262 de esta Ley;</p> <p>XLVII. Producción nacional: Contenido o programación generada por persona física o moral con financiamiento mayoritario de origen mexicano;</p> <p>XLVIII. Productor nacional independiente de contenidos audiovisuales: Persona física o moral de nacionalidad mexicana que produce obras audiovisuales a nivel nacional, regional o local, que no cuenta con una</p>	<p>XLIV. Política de inclusión digital universal: Conjunto de programas y estrategias emitidos por el Ejecutivo Federal orientadas a brindar acceso a las tecnologías de la información y la comunicación, incluyendo el Internet de banda ancha para toda la población, haciendo especial énfasis en sus sectores más vulnerables, con el propósito de cerrar la brecha digital existente entre individuos, hogares, empresas y áreas geográficas de distinto nivel socioeconómico, respecto a sus oportunidades de acceso a las tecnologías referidas y el uso que hacen de éstas;</p> <p>XLV. Portabilidad: Derecho de los usuarios de conservar el mismo número telefónico al cambiarse de concesionario o prestador de servicio;</p> <p>XLVI. Posiciones orbitales geoestacionarias: Ubicaciones en una órbita circular que se encuentran en el plano ecuatorial, que permiten que un satélite mantenga un periodo de traslación igual al periodo de rotación de la Tierra;</p> <p>XLVII. Preponderancia: Calidad determinada por el Instituto de un agente económico en los términos del artículo 262 de esta Ley;</p> <p>XLVIII. Producción nacional: Contenido o programación generada por persona física o moral con financiamiento mayoritario de origen mexicano;</p>
--	--

<p>concesión de telecomunicaciones o radiodifusión, ni es controlado por un concesionario en virtud de su poder de mando;</p> <p><b>XLIX. PROFECO:</b> La Procuraduría Federal del Consumidor;</p> <p><b>L. Programación de oferta de productos:</b> La que, en el servicio de radio y televisión tiene por objeto ofrecer o promover la venta de bienes o la prestación de servicios y cuya duración es superior a cinco minutos continuos;</p> <p><b>LI. Programador nacional independiente:</b> Persona física o moral que no es objeto de control por parte de algún concesionario de radiodifusión o por alguna afiliada, filial o subsidiaria de éste, ni es controlado por un concesionario en virtud de su poder de mando, que cuenta con la capacidad de conformar un canal de programación con base en estructura programática formada mayoritariamente por producción propia y producción nacional independiente y cuya titularidad sobre los derechos de autor sea mayoritariamente mexicana;</p> <p><b>LII. Punto de interconexión:</b> Punto físico o virtual donde se establece la interconexión entre redes públicas de telecomunicaciones para el intercambio de tráfico de interconexión o de tráfico de servicios mayoristas;</p>	<p><b>XLIX. Productor nacional independiente de contenidos audiovisuales:</b> Persona física o moral de nacionalidad mexicana que produce obras audiovisuales a nivel nacional, regional o local, que no cuenta con una concesión de telecomunicaciones o radiodifusión, ni es controlado por un concesionario en virtud de su poder de mando;</p> <p><b>L. PROFECO:</b> La Procuraduría Federal del Consumidor;</p> <p><b>LI. Programación de oferta de productos:</b> La que, en el servicio de radio y televisión tiene por objeto ofrecer o promover la venta de bienes o la prestación de servicios y cuya duración es superior a cinco minutos continuos;</p> <p><b>LII. Programador nacional independiente:</b> Persona física o moral que no es objeto de control por parte de algún concesionario de radiodifusión o por alguna afiliada, filial o subsidiaria de</p>
--	--

<p>LIII. Radiocomunicación: Toda telecomunicación o radiodifusión que es transmitida por ondas del espectro radioeléctrico;</p> <p>LIV. Radiodifusión: Propagación de ondas electromagnéticas de señales de audio o de audio y video asociado, haciendo uso, aprovechamiento o explotación de las bandas de frecuencia del espectro radioeléctrico, incluidas las asociadas a recursos orbitales, atribuidas por el Instituto a tal servicio, con el que la población puede recibir de manera directa y gratuita las señales de su emisor utilizando los dispositivos idóneos para ello;</p> <p>LV. Recursos orbitales: Posiciones orbitales geoestacionarias u órbitas satelitales con sus respectivas bandas de frecuencias asociadas que pueden ser objeto de concesión;</p> <p>LVI. Red compartida mayorista: Red pública de telecomunicaciones</p>	<p>éste, ni es controlado por un concesionario en virtud de su poder de mando, que cuenta con la capacidad de conformar un canal de programación con base en estructura programática formada mayoritariamente por producción propia y producción nacional independiente y cuya titularidad sobre los derechos de autor sea mayoritariamente mexicana;</p> <p>LIII. Punto de interconexión: Punto físico o virtual donde se establece la interconexión entre redes públicas de telecomunicaciones para el intercambio de tráfico de interconexión o de tráfico de servicios mayoristas;</p> <p>LIV. Radiocomunicación: Toda telecomunicación o radiodifusión que es transmitida por ondas del espectro radioeléctrico;</p> <p>LV. Radiodifusión: Propagación de ondas electromagnéticas de señales de audio o de audio y video asociado, haciendo uso, aprovechamiento o explotación de las bandas de frecuencia del espectro radioeléctrico, incluidas las asociadas a recursos orbitales, atribuidas por el Instituto a tal servicio, con el que la población puede recibir de manera directa y gratuita las señales de su emisor utilizando los dispositivos idóneos para ello;</p>
---	---

<p>destinada exclusivamente a comercializar capacidad, infraestructura o servicios de telecomunicaciones al mayoreo a otros concesionarios o comercializadoras;</p> <p>LVII. Red de telecomunicaciones: Sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;</p> <p>LVIII. Red pública de telecomunicaciones: Red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios, ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;</p> <p>LIX. Satélite: Objeto colocado en una órbita satelital, provisto de una estación espacial con sus frecuencias asociadas que le permite recibir, transmitir o retransmitir señales de radiocomunicación desde o hacia estaciones terrenas u otros satélites;</p> <p>LX. Secretaría: La Secretaría de Comunicaciones y Transportes;</p>	<p><b>LVI.</b> Recursos orbitales: Posiciones orbitales geoestacionarias u órbitas satelitales con sus respectivas bandas de frecuencias asociadas que pueden ser objeto de concesión;</p> <p><b>LVII.</b> Red compartida mayorista: Red pública de telecomunicaciones destinada exclusivamente a comercializar capacidad, infraestructura o servicios de telecomunicaciones al mayoreo a otros concesionarios o comercializadoras;</p> <p><b>LVIII.</b> Red de telecomunicaciones: Sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;</p> <p><b>LIX.</b> Red pública de telecomunicaciones: Red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios, ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;</p> <p><b>LX.</b> Satélite: Objeto colocado en una órbita satelital, provisto de una estación espacial con sus frecuencias asociadas</p>
--	---

<p>LXI. Servicio de usuario visitante: El servicio a través del cual los usuarios de una red pública de telecomunicaciones de servicio local móvil, pueden originar o recibir comunicaciones de voz o datos a través de la infraestructura de acceso de otro concesionario de red pública de telecomunicaciones del servicio local móvil, sin necesidad de realizar algún procedimiento adicional, al tratarse de usuarios de otra región local móvil o al estar fuera de la zona de cobertura de su proveedor de servicios móviles;</p> <p>LXII. Servicio mayorista de telecomunicaciones: Servicio de telecomunicaciones que consiste en el suministro de acceso a elementos individuales, a capacidades de una red o servicios, incluyendo los de interconexión, que son utilizados por concesionarios o comercializadores para proveer servicios de telecomunicaciones a los usuarios finales;</p> <p>LXIII. Servicios de interconexión: Los que se prestan entre concesionarios de servicios de telecomunicaciones, para realizar la interconexión entre sus redes e incluyen, entre otros, la conducción de tráfico, su originación y terminación, enlaces de transmisión, señalización, tránsito, puertos de acceso, ubicación, la compartición de infraestructura para interconexión, facturación y cobranza, así como otros servicios auxiliares de la misma y acceso a servicios;</p> <p>LXIV. Servicio de televisión y audio restringidos: Servicio de</p>	<p>que le permite recibir, transmitir o retransmitir señales de radiocomunicación desde o hacia estaciones terrenas u otros satélites;</p> <p>LXI. Secretaría: La Secretaría de Comunicaciones y Transportes;</p> <p>LXII. Servicio de usuario visitante: El servicio a través del cual los usuarios de una red pública de telecomunicaciones de servicio local móvil, pueden originar o recibir comunicaciones de voz o datos a través de la infraestructura de acceso de otro concesionario de red pública de telecomunicaciones del servicio local móvil, sin necesidad de realizar algún procedimiento adicional, al tratarse de usuarios de otra región local móvil o al estar fuera de la zona de cobertura de su proveedor de servicios móviles;</p> <p>LXIII. Servicio mayorista de telecomunicaciones: Servicio de telecomunicaciones que consiste en el suministro de acceso a elementos individuales, a capacidades de una red o servicios, incluyendo los de interconexión, que son utilizados por concesionarios o comercializadores para proveer servicios de telecomunicaciones a los usuarios finales;</p>
---	--

<p>telecomunicaciones de audio o de audio y video asociados que se presta a suscriptores, a través de redes públicas de telecomunicaciones, mediante contrato y el pago periódico de una cantidad preestablecida;</p>	<p><b>LXIV.</b> Servicios de interconexión: Los que se prestan entre concesionarios de servicios de telecomunicaciones, para realizar la interconexión entre sus redes e incluyen, entre otros, la conducción de tráfico, su originación y terminación, enlaces de transmisión, señalización, tránsito, puertos de acceso, coubicación, la compartición de infraestructura para interconexión, facturación y cobranza, así como otros servicios auxiliares de la misma y acceso a servicios;</p>
<p><b>LXV.</b> Servicios públicos de telecomunicaciones y radiodifusión: Servicios de interés general que prestan los concesionarios al público en general con fines comerciales, públicos o sociales de conformidad con lo dispuesto en la presente Ley y la Ley Federal de Competencia Económica;</p>	<p><b>LXV.</b> Servicio de televisión y audio restringidos: Servicio de telecomunicaciones de audio o de audio y video asociados que se presta a suscriptores, a través de redes públicas de telecomunicaciones, mediante contrato y el pago periódico de una cantidad preestablecida;</p>
<p><b>LXVI.</b> Sistema de comunicación por satélite: El que permite el envío de señales de radiocomunicación a través de una estación terrena transmisora a un satélite que las recibe, amplifica, procesa y envía de regreso a la Tierra para ser captada por una o varias estaciones terrenas receptoras;</p>	<p><b>LXVI.</b> Servicios públicos de telecomunicaciones y radiodifusión: Servicios de interés general que prestan los concesionarios al público en general con fines comerciales, públicos o sociales de conformidad con lo dispuesto en la presente Ley y la Ley Federal de Competencia Económica;</p>
<p><b>LXVII.</b> Sitio público: Para efectos de esta Ley y siempre que se encuentren a cargo de dependencias o entidades federales, estatales o municipales o bajo programas públicos de cualquiera de los tres órdenes de gobierno, se consideran como tal a:</p> <ul style="list-style-type: none"> <li>a. Escuelas, universidades y, en general, inmuebles destinados a la educación;</li> <li>b. Clínicas, hospitales, centros de salud y, en general, inmuebles para la atención de la salud;</li> </ul>	<p><b>LXVII.</b> Sistema de comunicación por satélite: El que permite el envío de señales de radiocomunicación a través de una estación terrena transmisora a un satélite que las recibe, amplifica, procesa y envía de regreso a la Tierra para ser captada por una o varias estaciones terrenas receptoras;</p>

- c. Oficinas de los distintos órdenes de gobierno;
- d. Centros comunitarios;
- e. Espacios abiertos tales como plazas, parques, centros deportivos y áreas públicas de uso común para la población en general, cuya construcción o conservación está a cargo de autoridades federales, estatales, municipales o del Distrito Federal;
- f. Aquellos que participen en un programa público, y
- g. Los demás que se consideren sitios públicos de acuerdo a la legislación vigente;

**LXVIII.** Telecomunicaciones: Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión;

**LXVIII.** Sitio público: Para efectos de esta Ley y siempre que se encuentren a cargo de dependencias o entidades federales, estatales o municipales o bajo programas públicos de cualquiera de los tres órdenes de gobierno, se consideran como tal a:

- a. Escuelas, universidades y, en general, inmuebles destinados a la educación;
- b. Clínicas, hospitales, centros de salud y, en general, inmuebles para la atención de la salud;

<p>LXIX. Tráfico: Datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que circulan por una red de telecomunicaciones;</p> <p>LXX. Valor mínimo de referencia: Cantidad expresada en dinero, misma que será considerada como el valor mínimo que se deberá pagar como contraprestación por la adjudicación de la concesión, y</p> <p>LXXI. Usuario final: Persona física o moral que utiliza un servicio de telecomunicaciones como destinatario final.</p>	<p>c. Oficinas de los distintos órdenes de gobierno;</p> <p>d. Centros comunitarios;</p> <p>e. Espacios abiertos tales como plazas, parques, centros deportivos y áreas públicas de uso común para la población en general, cuya construcción o conservación está a cargo de autoridades federales, estatales, municipales o del Distrito Federal;</p> <p>f. Aquellos que participen en un programa público, y</p> <p>g. Los demás que se consideren sitios públicos de acuerdo a la legislación vigente;</p> <p><b>LXIX.</b> Telecomunicaciones: Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión;</p> <p><b>LXX.</b> Tráfico: Datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que circulan por una red de telecomunicaciones;</p> <p><b>LXXI.</b> Valor mínimo de referencia: Cantidad expresada en dinero, misma que será considerada como el valor mínimo que se deberá pagar como</p>
--	---

<p>...</p> <p>Artículo 190. ...</p> <p>I a la XI. ...</p> <p>XII. Realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Los concesionarios que operen redes públicas de telecomunicaciones podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones. Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Instituto, al Congreso de la Unión y al Ejecutivo Federal.</p> <p>...</p>	<p>contraprestación por la adjudicación de la concesión, y</p> <p><b>LXXII.</b> Usuario final: Persona física o moral que utiliza un servicio de telecomunicaciones como destinatario final.</p> <p>...</p> <p><b>Artículo 190.</b> ...</p> <p>I a la XI. ...</p> <p><b>XII.</b> Realizar bajo la coordinación del Instituto, <b>y en su caso, con la colaboración del Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública</b> los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Los concesionarios que operen redes públicas de telecomunicaciones podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones. Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Instituto, al Congreso de la Unión y al Ejecutivo Federal.</p> <p>...</p>
--	--

**Ley General de Protección Civil.**

TEXTO VIGENTE	TEXTO PROPUESTO
<p>Artículo 2. ...</p> <p>I. a la XXXV. ...</p> <p>XXXVI. Mitigación: Es toda acción orientada a disminuir el impacto o daños ante la presencia de un agente perturbador sobre un agente afectable;</p> <p>XXXVII. Peligro: Probabilidad de ocurrencia de un agente perturbador potencialmente dañino de cierta intensidad, durante un cierto periodo y en un sitio determinado;</p> <p>XXXVIII. Preparación: Actividades y medidas tomadas anticipadamente para asegurar una respuesta eficaz ante el impacto de un fenómeno perturbador en el corto, mediano y largo plazo;</p> <p>XXXIX. Prevención: Conjunto de acciones y mecanismos implementados con antelación a la ocurrencia de los agentes perturbadores, con la finalidad de conocer los peligros o los riesgos, identificarlos, eliminarlos o reducirlos; evitar o mitigar su impacto destructivo sobre las personas, bienes, infraestructura, así como anticiparse a los procesos sociales de construcción de los mismos;</p> <p>XL. Previsión: Tomar conciencia de los riesgos que pueden causarse y las necesidades para enfrentarlos a través de las etapas de identificación de riesgos, prevención, mitigación, preparación, atención de emergencias, recuperación y reconstrucción;</p>	<p>Artículo 2. ...</p> <p>I. a la XXXV. ...</p> <p><b>XXXVI. ISINISP.- Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;</b></p> <p>XXXVII. Mitigación: Es toda acción orientada a disminuir el impacto o daños ante la presencia de un agente perturbador sobre un agente afectable;</p> <p>XXXVIII. Peligro: Probabilidad de ocurrencia de un agente perturbador potencialmente dañino de cierta intensidad, durante un cierto periodo y en un sitio determinado;</p> <p>XXXIX. Preparación: Actividades y medidas tomadas anticipadamente para asegurar una respuesta eficaz ante el impacto de un fenómeno perturbador en el corto, mediano y largo plazo;</p> <p>XL. Prevención: Conjunto de acciones y mecanismos implementados con antelación a la ocurrencia de los agentes perturbadores, con la finalidad de conocer los peligros o los riesgos, identificarlos, eliminarlos o reducirlos; evitar o mitigar su impacto destructivo sobre las personas, bienes, infraestructura, así como anticiparse a</p>

<p> <b>XLII. Programa Interno de Protección Civil:</b> Es un instrumento de planeación y operación, circunscrito al ámbito de una dependencia, entidad, institución u organismo del sector público, privado o social; que se compone por el plan operativo para la Unidad Interna de Protección Civil, el plan para la continuidad de operaciones y el plan de contingencias, y tiene como propósito mitigar los riesgos previamente identificados y definir acciones preventivas y de respuesta para estar en condiciones de atender la eventualidad de alguna emergencia o desastre;         </p> <p> <b>XLIII. Programa Nacional:</b> Al Programa Nacional de Protección Civil;         </p> <p> <b>XLIII. Protección Civil:</b> Es la acción solidaria y participativa, que en consideración tanto de los riesgos de origen natural o antrópico como de los efectos adversos de los agentes perturbadores, prevé la coordinación y concertación de los sectores público, privado y social en el marco del Sistema Nacional, con el fin de crear un conjunto de disposiciones, planes, programas, estrategias, mecanismos y recursos         </p>	<p>           los procesos sociales de construcción de los mismos         </p> <p> <b>XLII. Previsión:</b> Tomar conciencia de los riesgos que pueden causarse y las necesidades para enfrentarlos a través de las etapas de identificación de riesgos, prevención, mitigación, preparación, atención de emergencias, recuperación y reconstrucción;         </p> <p> <b>XLII. Programa Interno de Protección Civil:</b> Es un instrumento de planeación y operación, circunscrito al ámbito de una dependencia, entidad, institución u organismo del sector público, privado o social; que se compone por el plan operativo para la Unidad Interna de Protección Civil, el plan para la continuidad de operaciones y el plan de contingencias, y tiene como propósito mitigar los riesgos previamente identificados y definir acciones preventivas y de respuesta para estar en condiciones de atender la eventualidad de alguna emergencia o desastre;         </p> <p> <b>XLIII. Programa Nacional:</b> Al Programa Nacional de Protección Civil;         </p>
--	---

<p>para que de manera corresponsable, y privilegiando la Gestión Integral de Riesgos y la Continuidad de Operaciones, se apliquen las medidas y acciones que sean necesarias para salvaguardar la vida, integridad y salud de la población, así como sus bienes; la infraestructura, la planta productiva y el medio ambiente;</p>	
<p><b>XLIV. Reconstrucción:</b> La acción transitoria orientada a alcanzar el entorno de normalidad social y económica que prevalecía entre la población antes de sufrir los efectos producidos por un agente perturbador en un determinado espacio o jurisdicción. Este proceso debe buscar en la medida de lo posible la reducción de los riesgos existentes, asegurando la no generación de nuevos riesgos y mejorando para ello las condiciones preexistentes;</p>	<p><b>XLIV. Protección Civil:</b> Es la acción solidaria y participativa, que en consideración tanto de los riesgos de origen natural o antrópico como de los efectos adversos de los agentes perturbadores, prevé la coordinación y concertación de los sectores público, privado y social en el marco del Sistema Nacional, con el fin de crear un conjunto de disposiciones, planes, programas, estrategias, mecanismos y recursos para que de manera corresponsable, y privilegiando la Gestión Integral de Riesgos y la Continuidad de Operaciones, se apliquen las medidas y acciones que sean necesarias para salvaguardar la vida, integridad y salud de la población, así como sus bienes; la infraestructura, la planta productiva y el medio ambiente;</p>
<p><b>XLV. Recuperación:</b> Proceso que inicia durante la emergencia, consistente en acciones encaminadas al retorno a la normalidad de la comunidad afectada;</p>	<p><b>XLV. Reconstrucción:</b> La acción transitoria orientada a alcanzar el entorno de normalidad social y económica que prevalecía entre la población antes de sufrir los efectos producidos por un agente perturbador en un determinado espacio o jurisdicción. Este proceso debe buscar en la medida de lo posible la reducción de los riesgos existentes, asegurando la no generación de nuevos riesgos y mejorando para ello las condiciones preexistentes;</p>
<p><b>XLVI. Reducción de Riesgos:</b> Intervención preventiva de individuos,</p>	

instituciones y comunidades que nos permite eliminar o reducir, mediante acciones de preparación y mitigación, el impacto adverso de los desastres. Contempla la identificación de riesgos y el análisis de vulnerabilidades, resiliencia y capacidades de respuesta, el desarrollo de una cultura de la protección civil, el compromiso público y el desarrollo de un marco institucional, la implementación de medidas de protección del medio ambiente, uso del suelo y planeación urbana, protección de la infraestructura crítica, generación de alianzas y desarrollo de instrumentos financieros y transferencia de riesgos, y el desarrollo de sistemas de alertamiento;

**XLVII. Refugio Temporal:** La instalación física habilitada para brindar temporalmente protección y bienestar a las personas que no tienen posibilidades inmediatas de acceso a una habitación segura en caso de un riesgo inminente, una emergencia, siniestro o desastre;

**XLVIII. Resiliencia:** Es la capacidad de un sistema, comunidad o sociedad potencialmente expuesta a un peligro para resistir, asimilar, adaptarse y recuperarse de sus efectos en un corto plazo y de manera eficiente, a través de la preservación y restauración de sus

**XLVI. Recuperación:** Proceso que inicia durante la emergencia, consistente en acciones encaminadas al retorno a la normalidad de la comunidad afectada;

**XLVII. Reducción de Riesgos:** Intervención preventiva de individuos, instituciones y comunidades que nos permite eliminar o reducir, mediante acciones de preparación y mitigación, el impacto adverso de los desastres. Contempla la identificación de riesgos y el análisis de vulnerabilidades, resiliencia y capacidades de respuesta, el desarrollo de una cultura de la protección civil, el compromiso público y el desarrollo de un marco institucional, la implementación de medidas de protección del medio ambiente, uso del suelo y planeación urbana, protección de la infraestructura crítica, generación de alianzas y desarrollo de instrumentos financieros y transferencia de riesgos, y el desarrollo de sistemas de alertamiento;

**XLVIII. Refugio Temporal:** La instalación física habilitada para brindar temporalmente protección y bienestar a las personas que no tienen posibilidades inmediatas de acceso a

<p>estructuras básicas y funcionales, logrando una mejor protección futura y mejorando las medidas de reducción de riesgos;</p> <p>XLIX. Riesgo: Daños o pérdidas probables sobre un agente afectable, resultado de la interacción entre su vulnerabilidad y la presencia de un agente perturbador;</p> <p>L. Riesgo Inminente: Aquel riesgo que según la opinión de una instancia técnica especializada, debe considerar la realización de acciones inmediatas en virtud de existir condiciones o altas probabilidades de que se produzcan los efectos adversos sobre un agente afectable;</p> <p>LI. Secretaría: La Secretaría de Gobernación del Gobierno Federal;</p> <p>LII. Seguro: Instrumento de Administración y Transferencia de Riesgos;</p> <p>LIII. Simulacro: Representación mediante una simulación de las acciones de respuesta previamente planeadas con el fin de observar, probar y corregir una respuesta eficaz ante posibles situaciones reales de emergencia o desastre. Implica el</p>	<p>una habitación segura en caso de un riesgo inminente, una emergencia, siniestro o desastre;</p> <p>XLIX. Resiliencia: Es la capacidad de un sistema, comunidad o sociedad potencialmente expuesta a un peligro para resistir, asimilar, adaptarse y recuperarse de sus efectos en un corto plazo y de manera eficiente, a través de la preservación y restauración de sus estructuras básicas y funcionales, logrando una mejor protección futura y mejorando las medidas de reducción de riesgos;</p> <p>L. Riesgo: Daños o pérdidas probables sobre un agente afectable, resultado de la interacción entre su vulnerabilidad y la presencia de un agente perturbador;</p> <p>LI. Riesgo Inminente: Aquel riesgo que, según la opinión de una instancia técnica especializada, debe considerar la realización de acciones inmediatas en virtud de existir condiciones o altas probabilidades de que se produzcan los efectos adversos sobre un agente afectable;</p> <p>LII. Secretaría: La Secretaría de Gobernación del Gobierno Federal;</p> <p>LIII. Seguro: Instrumento de Administración y Transferencia de Riesgos;</p>
--	--

montaje de un escenario en terreno específico, diseñado a partir de la identificación y análisis de riesgos y la vulnerabilidad de los sistemas afectables;

LIV. Sistema Nacional: El Sistema Nacional de Protección Civil;

LV. Siniestro: Situación crítica y dañina generada por la incidencia de uno o más fenómenos perturbadores en un inmueble o instalación afectando a su población y equipo, con posible afectación a instalaciones circundantes;

LVI. Unidad Interna de Protección Civil: El órgano normativo y operativo responsable de desarrollar y dirigir las acciones de protección civil, así como elaborar, actualizar, operar y vigilar el Programa Interno de Protección Civil en los inmuebles e instalaciones fijas y móviles de una dependencia, institución o entidad perteneciente a los sectores público, privado y social; también conocidas como Brigadas Institucionales de Protección Civil;

LVII. Unidades de Protección Civil: Los organismos de la administración pública de las entidades federativas, municipales o de las delegaciones, encargados de la organización, coordinación y operación del Sistema Nacional, en su demarcación territorial;

LIV. Simulacro: Representación mediante una simulación de las acciones de respuesta previamente planeadas con el fin de observar, probar y corregir una respuesta eficaz ante posibles situaciones reales de emergencia o desastre. Implica el montaje de un escenario en terreno específico, diseñado a partir de la identificación y análisis de riesgos y la vulnerabilidad de los sistemas afectables;

LV. Sistema Nacional: El Sistema Nacional de Protección Civil;

LVI. Siniestro: Situación crítica y dañina generada por la incidencia de uno o más fenómenos perturbadores en un inmueble o instalación afectando a su población y equipo, con posible afectación a instalaciones circundantes;

LVII. Unidad Interna de Protección Civil: El órgano normativo y operativo responsable de desarrollar y dirigir las acciones de protección civil, así como elaborar, actualizar, operar y vigilar el Programa Interno de Protección Civil en

<p>LVIII. Vulnerabilidad: Susceptibilidad o propensión de un agente afectable a sufrir daños o pérdidas ante la presencia de un agente perturbador, determinado por factores físicos, sociales, económicos y ambientales;</p> <p>LIX. Zona de Desastre: Espacio territorial determinado en el tiempo por la declaración formal de la autoridad competente, en virtud del desajuste que sufre en su estructura social, impidiéndose el cumplimiento normal de las actividades de la comunidad. Puede involucrar el ejercicio de recursos públicos a través del Fondo de Desastres;</p> <p>LX. Zona de Riesgo: Espacio territorial determinado en el que existe la probabilidad de que se produzca un daño, originado por un fenómeno perturbador, y</p> <p>LXI. Zona de Riesgo Grave: Asentamiento humano que se encuentra dentro de una zona de grave riesgo, originado por un posible fenómeno perturbador.</p>	<p>los inmuebles e instalaciones fijas y móviles de una dependencia, institución o entidad perteneciente a los sectores público, privado y social; también conocidas como Brigadas Institucionales de Protección Civil;</p> <p>LVIII. Unidades de Protección Civil: Los organismos de la administración pública de las entidades federativas, municipales o de las delegaciones, encargados de la organización, coordinación y operación del Sistema Nacional, en su demarcación territorial;</p> <p>LIX. Vulnerabilidad: Susceptibilidad o propensión de un agente afectable a sufrir daños o pérdidas ante la presencia de un agente perturbador, determinado por factores físicos, sociales, económicos y ambientales;</p> <p>LX. Zona de Desastre: Espacio territorial determinado en el tiempo por la declaración formal de la autoridad competente, en virtud del desajuste que sufre en su estructura social, impidiéndose el cumplimiento normal de las actividades de la comunidad. Puede involucrar el ejercicio de recursos públicos a través del Fondo de Desastres;</p> <p>LXI. Zona de Riesgo: Espacio territorial determinado en el que existe la probabilidad de que se produzca un daño, originado por un fenómeno perturbador, y</p> <p>LXII. Zona de Riesgo Grave: Asentamiento humano que se encuentra dentro de una zona de grave</p>
--	--

<p>Artículo 16. ...</p> <p>Los integrantes del Sistema Nacional deberán compartir con la autoridad competente que solicite y justifique su utilidad, la información de carácter técnico, ya sea impresa, electrónica o en tiempo real relativa a los sistemas y/o redes de alerta, detección, monitoreo, pronóstico y medición de riesgos.</p> <p>Artículo 19. ...</p> <p>I. a la XXX. ...</p> <p>XXXI. Las demás que señalen los ordenamientos aplicables o que le atribuyan el Presidente o el Consejo Nacional dentro de la esfera de sus facultades.</p> <p>Artículo 21. ...</p> <p>...</p> <p><b>SIN CORRELATIVO</b></p>	<p>riesgo, originado por un posible fenómeno perturbador.</p> <p>Artículo 16. ...</p> <p>Los integrantes del Sistema Nacional deberán compartir con la autoridad competente que solicite y justifique su utilidad, la información de carácter técnico, ya sea impresa, electrónica o en tiempo real relativa a los sistemas y/o redes de alerta, detección, monitoreo, pronóstico y medición de riesgos. <b>En especial el ISINISP y los Complejos de Seguridad compartirán con el Sistema Nacional la información sobre emergencias que reciban, cuando impliquen la atención de dicho Sistema.</b></p> <p>Artículo 19. ...</p> <p>I. a la XXX. ...</p> <p><b>XXXI.- Establecer las bases de coordinación con el ISINISP, para los servicios que prestan los Centros de Supervisión y Control Regional de ese Instituto y los Complejos de Seguridad de las Entidades Federativas;</b></p> <p>XXXII. Las demás que señalen los ordenamientos aplicables o que le atribuyan el Presidente o el Consejo Nacional dentro de la esfera de sus facultades.</p> <p>Artículo 21. ...</p> <p>...</p> <p><b>Se atenderán los avisos de emergencia recibidos por los Complejos de Seguridad de la</b></p>
---	--

<p>...</p> <p>...</p> <p>...</p> <p>...</p>	<p><b>Entidades Federativas, de acuerdo con las bases establecidas conforme a la fracción XXXI del artículo 19 de esta Ley.</b></p> <p>...</p> <p>...</p> <p>...</p> <p>...</p>
<p>Artículo 24. ...</p>	
<p><b>SIN CORRELATIVO</b></p> <p>...</p> <p>...</p>	<p><b>Artículo 24. ...</b></p> <p><b>Recibirá y atenderá de manera prioritaria los avisos de emergencia de los Complejos de Seguridad de las Entidades Federativas, recibidos por estas instancias, determinando en primer lugar si dicha emergencia corresponde a la atención del Sistema o a otras instancias de atención de emergencias, incluyendo la de seguridad pública y, en su caso, procederá a su inmediato alertamiento a las instancias correspondientes del Sistema.</b></p> <p>...</p>

Por lo expuesto, someto a consideración de esta Cámara de Diputados el siguiente:

**Proyecto de decreto que expide la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública, y se reforman y adicionan diversas disposiciones de la Ley General del Sistema Nacional de Seguridad Pública; de la Ley del Sistema Nacional de Información Estadística y Geográfica; de la Ley de la Guardia Nacional; de la Ley Orgánica de la Fiscalía General de la República; de la Ley Federal de Telecomunicaciones y Radiocomunicación; y de la Ley General de Protección Civil.**

**Artículo Primero.** – Se expide la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública, para quedar como sigue:

# **“LEY NACIONAL DEL SISTEMA NACIONAL DE LA INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD PÚBLICA”**

## **TÍTULO PRIMERO DISPOSICIONES GENERALES**

**Artículo 1.-** La presente Ley, reglamentaria del párrafo 10 inciso b) del artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, es de orden público, de interés social y de observancia obligatoria para los Poderes de la Federación, los Estados y la CDMX; los Ayuntamientos de los Municipios; las Alcaldías de las demarcaciones territoriales de la Ciudad de México, y tiene por objeto regular:

- I. El Sistema Nacional de Información en Seguridad Pública;**
- II. La distribución de competencias y las bases de coordinación entre la Federación, las Entidades Federativas y los Municipios;**
- III. Las tecnologías de información y comunicaciones del Sistema;**
- IV. La organización y funcionamiento del Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública; y**
- V. Las especificaciones tecnológicas de la infraestructura de los Complejos de Seguridad y demás componentes del Sistema.**

**Artículo 2.-** Corresponde al Estado, por conducto del Instituto, las Entidades Federativas, los Municipios y las autoridades que resulten competentes, el control y la regulación de los actos inmersos en el objeto de la presente Ley, en los reglamentos correspondientes, normas oficiales mexicanas, normas técnicas y en las disposiciones que resulten aplicables.

Asimismo, corresponde al Estado, la propiedad y dominio pleno de la información contenida en las infraestructuras de información crítica y de información esenciales de seguridad pública, debido a ser parte de su soberanía y seguridad nacional, aun cuando se tengan sólo en calidad de posesión.

**Artículo 3.-** El Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública, contará para su funcionamiento y operación, con la finalidad, objetivos, principios, componentes, políticas y acciones previstos en la presente Ley.

**Artículo 4.-** La coordinación, evaluación y seguimiento de lo dispuesto en esta Ley, deberán llevarse a cabo con respeto a las atribuciones que la Constitución establece para las instituciones y autoridades que integran el Sistema.

**Artículo 5.- Para los efectos de esta Ley, se entenderá por:**

- I. Activos de TIC: los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos y además los de la infraestructura activa y pasiva de telecomunicaciones;**
- II. Acuerdo: el acuerdo de políticas y disposiciones para la EDN, en materia de TIC y en la de seguridad de la información, así como el Manual de Aplicación General en dichas materias;**
- III. Adquisición: a la obtención de las soluciones tecnológicas que cubran la totalidad de los requerimientos. Las adquisiciones podrán ser por compra directa, tercerización, arrendamiento o cualquier otra práctica;**
- IV. Alertamiento: al aviso por cualquier medio telefónico, fijo y móvil o mensajes por medio de cualquier instrumento tecnológico, incluidos aquellos que usen el espectro radioeléctrico y el internet;**
- V. Amenaza: a cualquier posible acto que pueda causar daño a las infraestructuras de información y comunicaciones y/o interrumpa los servicios de la institución;**
- VI. Análisis de riesgos: al método analítico de la gestión de riesgos, que permite la identificación de vulnerabilidades y amenazas de seguridad, así como la evaluación de la magnitud e impacto de los daños para determinar dónde será necesaria la implementación de controles o salvaguardas y estimar los recursos necesarios para eliminarlas o mitigarlas;**
- VII. APF: a la Administración Pública Federal;**
- VIII. Aplicativos de cómputo: el programa informático (software) y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo con requerimientos previamente definidos;**
- IX. Arquitectura tecnológica: a la estructura de equipamiento informático (hardware), programas informáticos (software) y redes requeridas para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la institución;**

- X. **Auditoría de seguridad de la información:** al análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que podrán presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicación o servidores;
- XI. **Auxilio:** a la respuesta de ayuda a las personas en riesgo o las víctimas de un siniestro, emergencia o desastre, prestadas por las corporaciones públicas y privadas responsables;
- XII. **Bases de datos nacionales:** las bases de datos que constituyen subconjuntos sistematizados de la información contenida en Registros Nacionales en materias relativas a detenciones, armamento, equipo y personal de seguridad pública, medidas cautelares, soluciones alternas y formas de terminación anticipada, así como las bases de datos del Ministerio Público y las instituciones policiales de los tres órdenes de gobierno relativas a la información criminalística, huellas dactilares de personas sujetas a un proceso o investigación penal, teléfonos celulares, personas sentenciadas y servicios de seguridad privada, así como las demás necesarias para la prevención, investigación y persecución de los delitos. El conjunto de bases de datos conformará el Sistema Nacional de Información;
- XIII. **Bases de datos:** al conjunto estructurado de datos, gestionado bajo el control de un ordenador de bases de datos, el cual se encarga de: controlar el acceso concurrente, evitar redundancia, cumplimiento de las restricciones y reglas de integridad, usar elemento que aceleren el acceso físico a los datos (índices, agrupamientos, funciones de dispersión, etc.), distribuir los bloques del disco del modo más adecuado para el crecimiento y uso de los datos, controlar el acceso y los privilegios de los usuarios y recuperar ante fallas, entre otros;
- XIV. **Cadena de custodia:** al Sistema de Control y Registro que se aplica al indicio, evidencia, objeto, instrumento, producto o imagen del hecho delictivo, desde su localización, descubrimiento o aportación, en el lugar de los hechos o del hallazgo, hasta que la autoridad competente ordene su conclusión;
- XV. **CDCR:** Centro de Datos de los Centros de Supervisión y Control Regional;
- XVI. **CDCS:** Centro de Datos Central del Sistema;

- XVII. CDCOS: Centro de Datos de los Complejos de Seguridad;**
- XVIII. Centro de datos: el lugar físico en los que se ubican los activos de TIC y desde el que se proveen servicios de TIC;**
- XIX. CSUCOR: al Centro de Supervisión y Control Regional;**
- XX. CNSP: al Consejo Nacional de Seguridad Pública;**
- XXI. Complejos de Seguridad: al órgano encargado de procesar información que permita realizar una respuesta a las diferentes situaciones que vive la ciudadanía en materia de seguridad. Este término engloba a las definiciones de un Centro de Control, Comando, Comunicación, Cómputo y Calidad y cualquier otro de índole similar;**
- XXII. Cómputo en la nube: al modelo de prestación de servicios digitales que permite a las instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura, de plataforma o de programas informáticos (software);**
- XXIII. Consejo Consultivo: al Consejo Consultivo Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;**
- XXIV. Convenios marco: a la estrategia de contratación basada en un acuerdo de voluntades que celebra una dependencia o entidad con uno o más posibles proveedores, mediante los cuales se establecen las especificaciones técnicas y de calidad, alcances, precios y condiciones que regularán la adquisición o arrendamiento de bienes muebles, o la prestación de servicios. Su objetivo principal es que estas contrataciones se realicen de manera ágil y en las mejores condiciones;**
- XXV. DOTIC: la Dirección Operativa de Administración auxiliada por las demás direcciones operativas y regionales;**
- XXVI. Dictamen técnico: al documento que suscribe el titular del área usuaria o solicitante de un bien o servicio de TIC, que forma parte de la requisición de compra, en el que se detalla el cumplimiento o el incumplimiento de cada uno de los requisitos técnicos establecidos en las bases de licitación o invitación, establecidos en el Título Sexto de esta Ley;**

- XXVII. Diseminación:** la transmisión o entrega de información considerada de seguridad nacional, de acuerdo con el nivel de acceso autorizado;
- XXVIII. Dominio tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la institución, los cuales podrán ser: los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, *internet*, intranet y aplicativos de cómputo, entre otros;
- XXIX. Donador:** al dispositivo necesario para garantizar la comunicación con otros estándares y/o protocolos y/o redes de banda ancha, y mantener el cifrado en todas las redes de radio;
- XXX. Drones:** a los vehículos aéreos no tripulados que se operan por control remoto empleado regularmente para servicios de vigilancia;
- XXXI. EDN:** la Estrategia Digital Nacional;
- XXXII. Emergencia:** a la situación anormal que puede causar un daño a la población al propiciar un riesgo excesivo a la vida y/o propiedad de las personas, generada o asociada con la inminencia, alta probabilidad o presencia de un fenómeno perturbador, antropogénico o natural, que puede ser fortuito o intencional;
- XXXIII. ERISC:** al equipo de respuesta a incidentes de seguridad en TIC en la institución;
- XXXIV. Especificaciones:** al conjunto de características cuantitativas y cualitativas que debe cumplir un proyecto en su producto final, ya sea un producto o servicio;
- XXXV. Estandarización o normalización:** al proceso de ajustar o adaptar características de los servicios y/o procedimientos de seguridad pública; con el objetivo de que éstos se asemejen a un tipo, modelo o norma en común;
- XXXVI. Equipamiento informático (hardware):** a los componentes físicos que conforman un equipo de cómputo;
- XXXVII. GPS:** al Sistema de Posicionamiento Global, por sus siglas en inglés;

- XXXVIII. Incidente:** a la afectación o interrupción de los servicios y/o de los activos de TIC, a las infraestructuras de información esenciales y/o críticas, así como a los activos de información de la institución, incluido el acceso no autorizado o no programado a estos;
- XXXIX. Infraestructura:** a los componentes que soportan los servicios informáticos y de comunicaciones, institucionales;
- XL. Infraestructura activa:** a los elementos de las redes de telecomunicaciones o radiodifusión que almacenan, emiten, procesan, reciben o transmiten escritos, imágenes, sonidos, señales, signos o información de cualquier naturaleza;
- XLI. Infraestructuras críticas de información:** a las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la seguridad nacional en términos de la Ley de la materia;
- XLII. Infraestructuras de información esenciales:** las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las instituciones;
- XLIII. Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar, y soportar los servicios de TIC;
- XLIV. Infraestructura pasiva:** elementos, accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como la prestación de servicios de procesamiento de datos, de telecomunicaciones y radio difusión;
- XLV. Instituto:** al Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;
- XLVI. Integridad:** la acción de mantener la exactitud y corrección de la información y sus métodos de proceso;
- XLVII. Interdependencia:** la interconexión estrecha que existe entre las infraestructuras de la información esenciales, y produce que la

falla o falta de una de ellas impacte negativamente en otras, presentándose como consecuencia un efecto cascada de fallas en la prestación de servicios;

- XLVIII. Interfases:** a las zonas de contacto o conexión entre dos elementos hardware o entre procesos;
- XLIX. Internet de las cosas:** al escenario en el que diversas cosas están conectadas y se comunican;
- L. Interoperabilidad:** la capacidad de organizaciones y sistemas, dispares y diversos para interactuar con objetivos consensuados y comunes con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las instituciones compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de TIC;
- LI. Ley:** a la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;
- LII. MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de TIC y en el de Seguridad de la Información. Anexo único del Acuerdo;
- LIII. Padrón de proveedores:** a la herramienta de carácter informático en el cual se realizará el registro o actualización de información por parte de las personas físicas o morales, nacionales o extranjeras, interesadas en participar en los procedimientos de licitación pública, invitación restringida a cuando menos tres proveedores y adjudicación directa; en materia de infraestructura de TIC e infraestructura activa y pasiva de redes de comunicaciones y que cuenten con número en el registro único de proveedores de CompraNet;
- LIV. Plan de contingencia:** al documento en el que se plantea la estrategia, el personal y el conjunto de actividades que se requieren para recuperar por completo o parcialmente un servicio, localidad o proceso crítico, en caso de que se presente un desastre. Dentro de este documento se establecen de igual manera las actividades, roles y responsabilidades para regresar a la normalidad una vez resuelto el incidente;
- LV. Precios de referencia:** herramienta que consiste en aquellos precios internos que fijan los compradores potenciales para poder usarlos como un precio estándar en la relación con los precios del mercado. En definitiva, son instrumentos que crea el consumidor

para poder elaborar juicios sobre el grado de aceptabilidad de los precios que observa.

El Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, prevé la posibilidad de que los compradores establezcan precios máximos de referencia a los que deberán sujetarse los proveedores de los bienes o servicios, fijando un porcentaje de descuento como parte de su proposición respecto de dichos precios;

- LVI. Procesamiento de datos:** a cualquier ordenación o tratamiento de datos (elementos básicos de información) que se lleva a cabo de manera automática por medio de sistemas o aplicativos de cómputo;
- LVII. Programa informático (Software):** al código, programa de código, conjunto de programas de código, procedimientos automatizados y rutinas de código que se asocian con la operación de equipo de cómputo y que tiene el propósito de ejecutar una función o proveer un servicio;
- LVIII. Red Nacional de Telecomunicaciones:** al sistema integrado por medios de transmisión, de voz, datos, video, radio, medios digitales, enlaces que utilicen bandas de frecuencia del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio; así como en su caso, centrales, dispositivos de comunicación o cualquier equipo necesario para los fines requeridos para la seguridad pública en toda la República Mexicana;
- LIX. Repositorio:** el espacio en medio magnético u óptico en el que se almacena y mantiene la información digital;
- LX. Riesgo:** a la probabilidad de que una amenaza aproveche la o las vulnerabilidades de un activo, así como las consecuencias de su impacto en una dependencia o entidad, es decir, daños o pérdidas probables sobre un agente afectable, resultado de la interacción entre su vulnerabilidad y la presencia de un agente perturbador;
- LXI. Secretaría:** a la Secretaría de Seguridad y Protección Ciudadana del Gobierno Federal;
- LXII. Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;

- LXIII. Seguridad:** a las acciones tendientes a garantizar la confidencialidad, integridad y disponibilidad de los activos;
- LXIV. Servidores:** a la computadora conectada a una red informática que contiene datos, programas, entre otros, que dan servicio a otras computadoras a través de esta red;
- LXV. Sistema Nacional de Seguridad Pública:** al Sistema a que se refiere la Ley General del Sistema Nacional de Seguridad Pública;
- LXVI. Sistema:** al Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;
- LXVII. Subsistema:** a la parte de un sistema que tiene por objeto procesos de conversión de las entradas y cuya estructura y funcionamiento tiene el comportamiento de un sistema, es decir son conjuntos estructurales sistémicos, susceptibles de ser aislados conceptualmente, por lo que son, elementos del sistema que, a su vez, son sistemas por derecho propio;
- LXVIII. STSP:** a las Soluciones de Tecnología para Seguridad Pública;
- LXIX. TIC:** las Tecnologías de la Información y Comunicaciones que comprenden el equipo de cómputo, software, dispositivos de impresión, infraestructura y servicios que sean utilizadas para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;
- LXX. Tecnologías verdes:** al conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las TIC, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;
- LXXI. Usuario:** a los servidores públicos o aquellos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC;
- LXXII. Vulnerabilidades:** a las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a las infraestructuras de información esenciales y/o críticas, así como a los activos de información; y

**LXXIII. Web Service:** a la aplicación de software que permite el intercambio de datos mediante un conjunto de estándares y protocolos para ser expuesta y consumida por otras aplicaciones del mismo tipo.

## **TÍTULO SEGUNDO DE LA DISTRIBUCIÓN DE COMPETENCIAS**

### **Capítulo I De la Federación**

**Artículo 6.-** Corresponde a la Federación por conducto de sus autoridades competentes:

- I. La creación y organización del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;**
- II. Establecer las acciones tendientes a asegurar la coordinación entre la Federación, las Entidades Federativas y los Municipios, a fin de garantizar el correcto funcionamiento del Sistema;**
- III. Proveer o determinar el origen de los recursos financieros y tecnológicos para la operación y creación del Sistema;**
- IV. Establecer la normatividad técnica para el funcionamiento de los servicios a que se refiere el artículo 13, así como realizar la planeación y programación globales del Sistema a través del Instituto, a fin de que sea un servicio público homogéneo para toda la población en el territorio nacional;**
- V. Encabezar, administrar, vigilar y operar el Sistema, a través del Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;**
- VI. Promover la coordinación y colaboración entre las corporaciones prestadoras de los servicios de auxilio públicas o privadas;**
- VII. Establecer los criterios para supervisar, por conducto del Instituto, el funcionamiento de los Complejos de Seguridad operados por las entidades federativas, sus dependencias o entidades;**
- VIII. Emitir los lineamientos generales para el funcionamiento de un organismo público descentralizado en las entidades federativas, que tendrá a su cargo la organización, control, operación y vigilancia de los Complejos de Seguridad;**

- IX. Vigilar, evaluar y certificar por conducto de los Centros de Supervisión y Control Regional del Instituto, las acciones operativas y funcionales de los Complejos de Seguridad;**
- X. Intervenir, a través del Instituto, en la dirección y operación de los Complejos de Seguridad, que incumplan las disposiciones previstas en éste u otros ordenamientos en la materia;**
- XI. Elaborar propuestas legislativas, ordenamientos administrativos o disposiciones técnicas de carácter obligatorio en materia de los servicios públicos objeto del Sistema, a través del Instituto;**
- XII. Controlar y resguardar las bases de datos que se generen por los procesos de prestación de los servicios en los Complejos de Seguridad, conforme al Reglamento de esta Ley;**
- XIII. Normar la planeación de nuevos Complejos de Seguridad, autorizar su creación y certificar su instalación y funcionamiento, a través del Instituto; y**
- XIV. Celebrar convenios con las corporaciones de prestación de auxilio privadas a través del Instituto, que serán el marco de referencia de los Convenios que podrán celebrar las Entidades Federativas con las corporaciones de auxilio locales.**

## **Capítulo II De las Entidades Federativas**

**Artículo 7.-** Corresponde a las Entidades Federativas en el ámbito de sus respectivas competencias:

- I. Crear un órgano local descentralizado de la administración pública de la entidad federativa, con autonomía de gestión para llevar a cabo la organización, control, vigilancia, funcionamiento y operación de sus Complejos de Seguridad;**
- II. Emitir el Reglamento correspondiente de los Complejos de Seguridad, con la intervención y asesoría del Instituto con objeto de armonizar su funcionamiento;**
- III. Establecer las directrices para armonizar el funcionamiento de los Complejos de Seguridad de su adscripción, supervisar su funcionamiento y asegurar su autonomía de las corporaciones de prestación de los servicios objeto de esta Ley;**

- IV. Llevar a cabo la supervisión de los Complejos de Seguridad por medio del organismo público descentralizado o de la Secretaría que determine cada Entidad Federativa, para el caso de contar con un solo Complejo de Seguridad para toda la Entidad Federativa;
- V. Proveer o determinar el origen de los recursos financieros, humanos, materiales, tecnológicos y todos aquellos que sirvan al órgano público descentralizado, para la instalación y operación de los Complejos de Seguridad bajo su responsabilidad;
- VI. Establecer las medidas necesarias para que las corporaciones prestadoras de la atención material de las emergencias, realicen los servicios solicitados por los Complejos de Seguridad, en forma eficaz y en el menor tiempo posible, proporcionando un reporte del cierre de cada servicio prestado;
- VII. Cumplir con los lineamientos establecidos y el Protocolo de registro de información establecidos por el Instituto para el CDCS, para que los Complejos de Seguridad registren en tiempo real la información generada para la conformación y conservación de las bases de datos de dicho Centro y del propio CDCOS;
- VIII. Vigilar que la operación y funcionamiento de los Complejos de Seguridad, cuenten con certificación y cumplan con la normatividad técnica correspondiente;
- IX. Proporcionar los terrenos para la instalación de las oficinas necesarias para el funcionamiento de los Centros de Supervisión y Control Regionales.
- X. Garantizar la seguridad y el resguardo de las instalaciones del Sistema de los órganos locales autónomos y de los Complejos de Seguridad; y
- XI. Asegurar el cumplimiento de lo previsto en, la presente ley, así como a los lineamientos, protocolos, reglamentos y normatividad que de ésta se derivan.

### **Capítulo III De los Municipios**

#### **Artículo 8.- Corresponde a los municipios:**

- I. Administrar y operar los Complejos de Seguridad que tengan establecidos y en su caso, transferir su operación al órgano descentralizado de su Entidad Federativa;

- II. Coordinar a las corporaciones de auxilio de su jurisdicción, a efecto de lograr una oportuna atención a los llamados generados por los Complejos de Seguridad de manera oportuna y en el menor tiempo posible;
- III. Proveer la seguridad y resguardo de las instalaciones de los Complejos de Seguridad localizados dentro de su territorio;
- IV. Proporcionar o determinar el origen y fuente de los recursos necesarios para la operación de los inmuebles requeridos para la construcción y puesta en operación de los Complejos de Seguridad; y
- V. Observar y dar cumplimiento a lo establecido en la presente ley, sus reglamentos, lineamientos y protocolos en materia de prestación de servicios que competen a los Complejos de Seguridad bajo su jurisdicción.

### **TÍTULO TERCERO**

#### **DEL SISTEMA NACIONAL DE LA INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD PÚBLICA**

##### **Capítulo I**

##### **De la Finalidad, Objetivos Naturaleza y Principios del Sistema**

**Artículo 9.-** El Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública, tendrá como finalidad suministrar a la sociedad y al Estado la información e interconexión tecnológica de calidad, pertinente, veraz y oportuna, a efecto de coadyuvar a los fines de la seguridad pública.

**Artículo 10.-** El Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública, tendrá como objetivos:

- I. Regular y operar la recopilación, almacenamiento y procesamiento de datos; y explotación y uso de la información para la seguridad pública;
- II. Integrar, controlar, actualizar y proteger las bases de datos nacionales de seguridad pública;
- III. Vigilar la operación de la Red Nacional de Telecomunicaciones y emitir los criterios estándares, protocolos y demás lineamientos para su interoperabilidad;

- IV. Regular la interconexión, interoperabilidad y protección de las bases de datos de información, entre las Entidades Federativas y los municipios, y generadas por ellos, requerida por la seguridad pública, con las limitaciones de esta prescritas por el Sistema;
- V. Emitir las normas, lineamientos, procedimientos, protocolos y criterios para la construcción y adquisición de activos, con particular énfasis de las limitaciones y resguardo que implican aquellos considerados como críticos, con el fin de garantizar su acceso y dominio pleno del Estado Mexicano;
- VI. Establecer la coordinación entre las instancias relacionadas con la información y comunicaciones y establecer las disposiciones reguladoras de los concesionarios de telecomunicaciones y de los prestadores de los servicios de auxilio; y
- VII. Los demás, que en el futuro pueda determinar el CNSP.

**Artículo 11.-** El Sistema por su naturaleza es un Sistema abierto, ya que, interactúa con su medio, importando materia-energía, transformando esa energía y exportando comunicación-información a ese medio, siendo sus características principales, las siguientes:

- I. Corriente de entrada: A través de la cual importan y reciben la energía necesaria para su funcionamiento;
- II. Proceso de conversión: Cambia elementos de entrada en información-comunicación organizada lo que les agrega valor a las salidas;
- III. Corriente de salida: Son los resultados del proceso de conversión del Sistema, que por ser positivos son útiles al medio -comunidad- ;
- IV. Elemento de retroalimentación: Genera información que indica como lo está haciendo el Sistema en la búsqueda de su objetivo y la introduce nuevamente, para hacer las correcciones necesarias.

**Artículo 12.-** Serán principios rectores del Sistema: los de accesibilidad; transparencia; legalidad; objetividad; eficiencia; promoción, respeto, protección y garantía de los derechos humanos; perspectiva de género e interculturalidad; paz y seguridad de la sociedad; fomento al desarrollo sustentable; la no discriminación; acceso a la información y protección de datos personales y el fomento de la participación ciudadana.

## **Capítulo II**

### **De los Componentes Básicos del Sistema**

**Artículo 13.-** Los servicios públicos objeto del Sistema, conforme a la Norma Técnica de Homologación de los Complejos de Seguridad, son los siguientes:

- a) Sistema de Atención de Llamadas de Emergencia a través de los números telefónicos 911, 088 y cualesquiera otros que se establezcan en el futuro;
- b) Sistemas de videovigilancia, públicos y privados interconectados;
- c) Sistema de Atención de Llamadas de Denuncia Anónima 089;
- d) Tecnologías emergentes: i) arcos lectores/aplicación móvil de reconocimiento de placas; ii) cámaras móviles; iii) aplicaciones móviles; iv) sensores/alarmas de pánico y botones de emergencia; y v) drones.
- e) Red de comunicaciones locales del Complejo de Seguridad;
- f) Área de inteligencia;
- g) Sistema de bases de datos: interoperabilidad interna del Complejo de Seguridad e interoperabilidad externa, con: I) Informe Policial Homologado; II) Licencias de conducir; III) Mandamientos judiciales; IV) Registro Nacional de Armamento y Equipos; v) Registro Nacional de Información Penitenciaria; vi) Registro Nacional de Personal de Seguridad Pública; VII) Registro de Vehículos Robados y Recuperados; VIII) Registro Público Vehicular; y IX) Incidencia delictiva;
- h) Red Nacional de Telecomunicaciones/redes estatales de transporte de datos, para la interoperabilidad del sistema;
- i) Red LAN: soporte de los servicios sustantivos y adjetivos; y
- j) Circuito Cerrado de Televisión.

**Artículo 14.-** Los ejes rectores para la regulación del Sistema son: Estandarización, Interoperabilidad, Homologación, Unificación, Coordinación y colaboración interinstitucional, Confidencialidad y respeto a la privacidad, y Transparencia de gestión.

**Artículo 15.-** Las instancias y sujetos del Sistema son:

- I. Consejo Nacional de Seguridad Pública;
- II. El Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;
- III. La Secretaría de Seguridad y Protección Ciudadana del gobierno federal.
- IV. Las instituciones de seguridad pública a que se refiere la fracción octava del artículo 5 de la Ley General del Sistema Nacional de Seguridad Pública;
- V. Los organismos autónomos federales y estatales, incluidos en estos a las fiscalías General de la República y de las Entidades Federativas;
- VI. Los organismos locales descentralizados de la administración pública de las Entidades Federativas responsables de la operación y funcionamiento de los Complejos de Seguridad y éstos últimos;
- VII. Todos los entes públicos de la federación, de las entidades federativas y municipales; y

- VIII. Sujetos privados: personas físicas y morales interconectadas con los integrantes de la Red Nacional de Telecomunicaciones para la seguridad pública.**

Los entes públicos a que se refiere este artículo regirán su actuación por los principios de: promoción, respeto, protección y garantía de los derechos humanos, universalidad, interdependencia, indivisibilidad, progresividad, accesibilidad, la no discriminación, acceso a la información, protección de datos personales, legalidad, objetividad, eficiencia, honradez, perspectiva de género e interculturalidad, fomento al desarrollo sustentable, y paz y seguridad de la sociedad.

**Artículo 16.- Los instrumentos del Sistema son los considerados en los artículos 113 y 136 de esta Ley.**

**Artículo 17.- Los activos de TIC del Sistema son:**

- I. La infraestructura en materia de construcciones: del Instituto; los Complejos de Seguridad; las instalaciones fijas de la Red Nacional de Telecomunicaciones, y todas las construcciones que soportan la arquitectura tecnológica, para la seguridad pública;**
- II. Infraestructura de TIC para generar las bases nacionales de datos a que se refiere la fracción segunda del artículo 5 de la Ley General del Sistema Nacional de Seguridad Pública; de los Complejos de Seguridad y de las plataformas de servicios integradoras de carácter nacional;**
- III. Red Nacional de Telecomunicaciones para la seguridad pública, comprendidas su infraestructura activa y pasiva; y**
- IV. Infraestructuras críticas y esenciales de información comprendidas en las fracciones anteriores.**

### **Capítulo III De la Organización del Sistema**

**Artículo 18.- El Sistema estará integrado por:**

- I. El Consejo Consultivo Nacional;**
- II. Los subsistemas nacionales de: recopilación y almacenamiento de datos e información; procesamiento e integración de Bases de Datos; explotación, uso y diseminación de la información; e interoperabilidad y comunicaciones;**
- III. El Instituto, incluidos sus Centros de Supervisión y Control Regional, y los Complejos de Seguridad; y**

**IV. La Red Nacional de Telecomunicaciones.**

**Artículo 19.- El Consejo Consultivo Nacional, estará integrado por:**

- I. El Director General del Instituto;**
- II. El titular o representante de la Secretaría de Seguridad y Protección Ciudadana;**
- III. El titular o representante de la Coordinación Nacional de Protección Civil;**
- IV. El titular o representante de la Guardia Nacional;**
- V. Tres representantes nombrados por la Conferencia Nacional de Secretarios de Seguridad Pública;**
- VI. El titular o representante de la Secretaría de Salud;**
- VII. Los titulares o sus representantes de los: Instituto Federal de Telecomunicaciones; Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; y del Instituto Nacional de Estadísticas y Geografía.**
- VIII. El titular o representante del Fiscal General de la República;**
- IX. Tres representantes nombrados por la Conferencia Nacional de Procuración de Justicia; y**
- X. El titular o representante de la Comisión de Derechos Humanos.**

Los miembros del Consejo Consultivo Nacional duraran en su encargo dos años, pero sus representantes continuaran en funciones aún después de terminado su periodo, en tanto no sean elegidos los que deban sustituirlos.

Los integrantes del Consejo Consultivo Nacional desempeñaran sus funciones en dicho órgano colegiado de manera honoraria.

**Artículo 20.- El Consejo Consultivo Nacional deberá:**

- I. Emitir su opinión respecto de las propuestas y estudios que le presente la Junta de Gobierno, en relación con:**
  - a) Los instrumentos y políticas públicas en materia de información y comunicaciones;**
  - b) Las formas de coordinación de las instancias y sujetos participes en el Sistema;**
  - c) Políticas en materia de suministro, intercambio, sistematización y actualización de la información de seguridad pública;**
  - d) Los parámetros, indicadores y características mínimas de los activos de los Complejos de Seguridad y nodos de la Red Nacional de Telecomunicaciones;**
  - e) Dictámenes sobre los proyectos de adquisición de activos de tecnologías de información y comunicaciones;**
  - f) Mecanismos diseñados para que la sociedad participe en los procesos de evaluación de políticas y acciones de información y comunicaciones para la seguridad pública;**

- g) Políticas de coordinación y colaboración con el Poder Judicial de la Federación y los órganos jurisdiccionales de las Entidades Federativas.
- II. Proponer y en su caso analizar los temas, información, comunicación e indicadores, sobre la información y comunicaciones que deben considerarse de interés nacional o de carácter crítico;
  - III. Analizar las propuestas de la Junta de Gobierno para la creación de nuevos subsistemas;
  - IV. Opinar sobre los demás asuntos que someta a su consideración la Junta de Gobierno.

**Artículo 21.-** El Consejo Consultivo Nacional será presidido por el director general del Instituto y fungirá como secretario técnico el servidor público del Instituto que aquel determine.

El Consejo se reunirá de manera ordinaria al menos una vez cada semestre, y en forma extraordinaria cuando la naturaleza de algún asunto de su competencia así lo exija.

La convocatoria será formulada por el director general del Instituto o a solicitud de al menos 25% de los miembros del Consejo, con el objeto de tratar algunos de los asuntos a que se hace referencia en el artículo 20 de esta Ley.

La convocatoria deberá hacerse con la anticipación necesaria, según la naturaleza y urgencia de los asuntos a tratar. Las reuniones se desahogarán conforme a las reglas que se adopten, a propuesta del Instituto.

#### **Capítulo IV** **De la Estructura Funcional del Sistema**

**Artículo 22.-** El Sistema contará con los siguientes Subsistemas Nacionales:

- I. Recopilación y almacenamiento de datos e información;
- II. Procesamiento e integración de Bases de Datos;
- III. Explotación, uso y disseminación de la información; e
- IV. Interoperabilidad y comunicaciones.

En todos estos Subsistemas se asegurará la continuidad funcional de la infraestructura y del acervo de información de TIC.

#### **Capítulo V** **Del Subsistema de Recopilación y Almacenamiento de Datos e Información**

**Artículo 23.-** Este subsistema tiene por objeto la recolección de datos a través de las siguientes fuentes:

**I. Fuentes fijas:**

- a) Llamadas de voz a través de los servicios telefónicos 911 y 088 (Guardia Nacional);
- b) Llamadas de voz, correos electrónicos y mensajes por redes sociales de la Denuncia Anónima 089;
- c) Imágenes a través del Sistema de Videovigilancia Públicos y Privados;
- d) Documentos del IPH e investigaciones;
- e) Datos a través del Sistema de Alarmas; y
- f) Datos de botones de pánico.

**II. Fuentes móviles:**

- a) Imágenes y datos provenientes de drones;
- b) Datos del Sistema de Rastreo Vehicular GPS;
- c) Llamadas de voz provenientes de patrullas; y
- d) Llamadas de voz, datos, imágenes provenientes de aplicaciones ciudadanas.

**Artículo 24.-** Este Subsistema se conforma de:

- I. Acervo de activos de TIC de las instancias institucionales que sustentan la operación de los servicios individuales; y
- II. Red Nacional de Centrales de Monitoreo de entidades reguladas por las normativas vigentes en materia de Seguridad Pública.

**Artículo 25.-** Este Subsistema se implementa, a través de:

- I. La comprobación de interoperabilidad con las Bases de Datos Nacionales; y
- II. Las entidades reguladas por la normativa de seguridad privada, configuradas como fuentes confiables de alertamiento.

**Artículo 26.-** Este Subsistema deberá contar con mecanismos y protocolos de “homologación de códigos”, tanto para la diversidad de formas físicas de los datos, como para la dispersión física y funcional de las fuentes y la diversidad de ámbitos y jurisdicciones institucionales, como para la transferencia de datos a través de la red de medios de comunicación, entre los sitios de recolección de datos y los centros de almacenamiento e integración de ellos, a fin de que dicha transferencia se haga con fidelidad de contenidos, rapidez e interoperabilidad.

**Artículo 27.-** El almacenamiento e integración de datos deberá realizarse en la infraestructura de TIC, en plataformas por fuentes e integradoras, para

asegurar la fidelidad de contenidos, en una integración centralizada con particular cuidado en la cadena de custodia de imágenes, para transformarse en prueba plena en los procesos judiciales, lo que implica la unificación de procedimientos de operación con la debida confidencialidad y respetos a la privacidad de las personas.

## **Capítulo VI**

### **Del Subsistema de Procesamiento e Integración de Bases de Datos**

**Artículo 28.-** Este Subsistema tiene como objeto el procesamiento e integración de las bases de datos locales a las unidades integradoras de bases de datos nacionales.

**Artículo 29.-** La operación de este Subsistema implica la unificación de procedimientos de integración y accesos, procurando fidelidad de contenidos y rapidez de transferencia.

**Artículo 30.-** Este Subsistema debe contar con un procedimiento eficaz de restricciones de acceso, contemplando una ampliación de perfiles de acceso nominales a las bases de datos nacionales, para los integrantes del Sistema, bajo indicaciones puntuales.

**Artículo 31.-** El Subsistema, para la debida conservación de las bases de datos nacionales, deberá contar con mecanismos de seguridad de la información, para la protección y salvaguarda de contenidos en almacenamiento y transferencias, con particular seguridad para la cadena de custodia de imágenes y cualquier otro elemento que pueda servir como prueba en los procesos judiciales.

## **Capítulo VII**

### **Del Subsistema de Explotación, Uso y Diseminación de la Información**

**Artículo 32.-** Los aspectos de explotación y uso de la información, son al menos:

- I. Atención de emergencias;**
- II. Apoyo a operativos ministeriales, judiciales y policiales;**
- III. Prevención de delitos;**
- IV. Inteligencia policial para efectos de prospección;**
- V. Investigación de delitos;**
- VI. Soporte a procesos judiciales a través de indicios y evidencias;**
- VII. Formulación de políticas públicas.**

**Artículo 33.-** Los requisitos esenciales para la operación de este Subsistema, son:

- I. **Comprobación de interoperabilidad con las bases de datos nacionales;**
- II. **Acceso restringido a las bases de datos nacionales; y**
- III. **Acceso directo a las bases de datos nacionales por parte de los integrantes del Sistema, con apego a los controles y restricciones establecidos.**

**Artículo 34.-** La clasificación, protección y diseminación de la información esencial y crítica de seguridad nacional que corresponda establecer y regular al Instituto, será aprobada por su Junta de Gobierno a propuesta del director general y previa opinión del Consejo Consultivo Nacional, con sujeción a las disposiciones de la Ley de Seguridad Nacional y de la Ley Federal de Transparencia y Acceso a la Información Pública.

#### **Capítulo VIII**

##### **Del Subsistema de Interoperabilidad y Comunicaciones**

**Artículo 35.-** Este subsistema tiene como objeto regular la conformación, implementación, operación y seguridad de la transferencia de datos e información.

**Artículo 36.-** En este subsistema se regula a la Red Nacional de Telecomunicaciones, por lo que hace tanto a su infraestructura activa como pasiva, a las redes locales interconectadas a la misma y a toda la información generada en TIC, tanto esencial como crítica, para Seguridad Pública.

**Artículo 37.-** La transferencia de datos que se realice a través de la red de medios de comunicación entre los sitios de recolección de datos y los centros de almacenamiento e integración de datos e información, y de estos a los puntos de uso y en su caso diseminación, deberá asegurar la fidelidad de contenidos y la celeridad de la transferencia. Estas redes podrán ser de medios dedicados –canales permanentes seguros de acceso cerrado– y de medios no dedicados –canales esporádicos a través de acceso abierto–.

**Artículo 38.-** La transferencia de las fuentes de datos a las bases de datos locales ubicadas, en los Centros de Supervisión y Control Regional y en los Complejos de Seguridad del Sistema, deberán sujetarse a las disposiciones generales para la seguridad de la información y para aquellas consideradas de Seguridad Nacional.

#### **Capítulo IX**

##### **De las Disposiciones Regulatoras de los Concesionarios de Telecomunicación y de los Prestadores de Servicios de Auxilio**

**Artículo 39.-** Los concesionarios de los servicios de Telecomunicaciones, estarán obligados a cursar las llamadas o alertas que por cualquier medio realicen los usuarios hacia los Complejos de Seguridad, de manera gratuita.

Asimismo, están obligados a proporcionar los datos del lugar de donde proviene la llamada o alerta, para identificar el número, la zona geográfica y los datos del titular de la línea o medio, para que la llamada o alerta sea canalizada al Complejo de Seguridad que corresponda. Los concesionarios deberán proporcionar al Complejo de Seguridad, el registro original de la llamada o alerta de emergencia.

Las obligaciones a que se refiere este artículo se complementarán y fundamentarán con las establecidas en los artículos 189, 190 y 190 bis de la Ley Federal de Telecomunicaciones y Radiodifusión.

**Artículo 40.-** Los prestadores de servicios de las corporaciones de auxilio, están obligados a colaborar y dar prioridad a las solicitudes que son canalizadas a través de los Complejos de Seguridad, empleando todos los recursos a su disposición con oportunidad, eficiencia y en el menor tiempo posible, manteniendo el intercambio de información a través de las plataformas tecnológicas, que permitan recibir prioritariamente las llamadas y adecuar los procesos internos de información y comunicación.

**Artículo 41.-** Los prestadores de servicios de las corporaciones de auxilio privadas, se obligarán a la prestación de sus servicios en los términos de los convenios o instrumentos específicos que suscriban con el Instituto.

**Artículo 42.-** Los prestadores de servicios de las corporaciones de auxilio públicas y privadas, estarán obligados al finalizar la actuación del evento, a reportar al Complejo de Seguridad que emitió la solicitud de auxilio, para fines de registro del cierre de la incidencia y para el debido funcionamiento de los sistemas de información y estadística.

**Artículo 43.-** Las corporaciones de auxilio comprenderán a: las autoridades de las fuerzas y cuerpos del Estado: Secretaría de la Defensa Nacional, Secretaría de Marina, Guardia Nacional; corporaciones de policías estatales y municipales; los hospitales y centros sanitarios públicos o privados; los servicios de vigilancia forestales; los de obras públicas, mantenimiento de carreteras, puentes nacionales o internacionales; los servicios de bomberos; los servicios de asistencia sanitaria extrahospitalarias públicos y privados; los servicios de emergencia de aeropuertos; los medios de transporte sanitarios dependientes de organismos públicos y privados; los servicios de empresas de seguridad privada debidamente registrados; el Sistema Nacional de Protección civil en cualquiera de sus organizaciones; los servicios de suministro, mantenimiento y conservación de redes de telecomunicaciones, telégrafos, agua, gas y electricidad; los grupos de salvamento y socorrismo

voluntarios de protección civil, salvamento marítimo y; todas aquellas organizaciones o agrupaciones tanto públicas como privadas, que se relacionen con la atención de emergencias.

## **TÍTULO CUARTO DEL INSTITUTO NACIONAL DEL SISTEMA DE LA INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD PÚBLICA**

### **Capítulo I Disposiciones Generales**

**Artículo 44.-** El Instituto es un organismo público descentralizado con autonomía técnica y de gestión, personalidad jurídica y patrimonio propios, responsable de normar, coordinar y operar el Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública.

**Artículo 45.-** El Instituto tendrá como objetivo implementar e instrumentar la finalidad y objetivos del Sistema, comprendidos en los artículos 9 y 10 de esta Ley, así como todas las acciones requeridas para lograr el mismo.

**Artículo 46.-** El Instituto tendrá como objetivos prioritarios, los siguientes:

- I. Asegurar el cumplimiento y garantizar que las unidades administrativas y su personal, tengan como código mínimo de ética y orientación de sus acciones, los principios establecidos para el Sistema en el artículo 12 de esta Ley; y
- II. Vigilar y consolidar el estricto cumplimiento de la normatividad, relativa al pleno dominio del Estado de las infraestructuras críticas y esenciales de información del Sistema.

**Artículo 47.-** El Instituto dirigirá y regulará la prestación de los servicios objeto del Sistema con base en los ejes rectores y mediante los instrumentos y activos de TIC, con los que cuente.

### **Capítulo II De su Organización y Funcionamiento**

#### **Sección I De las Funciones del Instituto**

**Artículo 48.-** El Instituto en su calidad de responsable y supervisor del Sistema, tendrá las siguientes funciones:

- I. Regular, conducir y coordinar el Sistema, así como fomentar las acciones que permitan mantener su operación eficiente;**
- II. Crear los subsistemas necesarios para el funcionamiento del Sistema, previa opinión favorable de su Consejo Consultivo Nacional;**
- III. Establecer y coordinar las actividades que lleven a cabo los subsistemas, tomando en cuenta los estándares nacionales e internacionales, así como las mejores prácticas en la materia;**
- IV. Solicitar a los subsistemas la información relativa a sus actividades, para el mejor funcionamiento y elaboración de políticas públicas;**
- V. Coordinar con el Instituto Federal de Telecomunicaciones las acciones necesarias para:**
  - a) El debido funcionamiento de la Red Nacional de Telecomunicaciones, así como para la adecuada participación de sus integrantes; y**
  - b) Que los concesionarios de telecomunicaciones aporten las tecnologías para la captación de datos, voz e imágenes.**
- VI. Llevar a cabo las acciones de coordinación con los prestadores de servicios de emergencia, tanto públicos como privados para:**
  - a. Unificar criterios y lograr la inmediata atención de dichas emergencias; y**
  - b. Le emisión de los protocolos y lineamientos básicos para su interconexión a los complejos de seguridad.**
- VII. Vigilar el cumplimiento de las disposiciones de carácter general, que se relacionen con el funcionamiento de los servicios públicos objeto del Sistema;**
- VIII. Promover y proveer el uso de definiciones técnicas, clasificaciones, nomenclaturas, abreviaturas, identificadores, directorios, símbolos, delimitaciones geográficas y demás elementos técnicos requeridos por los objetivos del Sistema, desde la etapa de captación hasta la de procesamiento y uso de la información, así como para el debido funcionamiento de la Red Nacional de Telecomunicaciones de conformidad con la Ley Federal sobre Metrología y Normalización;**
- IX. Llevar a cabo la supervisión y control de los Complejos de Seguridad ubicados en todo el territorio nacional y en su caso, intervenir la dirección y operación de aquel en el que se detecten irregularidades**

reiteradas, derivadas de la evaluación realizada para dicho subsistema;

- X. Desarrollar investigaciones e innovaciones científicas y tecnológicas en materia de Seguridad Pública;
- XI. Celebrar convenios marco con las corporaciones de auxilio privadas, los proveedores de bienes y servicios de TIC y las corporaciones privadas que se conecten a la Red Nacional de Telecomunicaciones para la seguridad pública;
- XII. Establecer los mecanismos y medidas necesarias para la seguridad de la información, Red Nacional de Telecomunicaciones y bases de datos nacionales, previstas en la fracción segunda del artículo 5 de la Ley General del Sistema Nacional de Seguridad Pública; y
- XIII. Las demás que le asigne el CNSP.

**Artículo 49.-** El Instituto realizará las supervisiones, revisiones y evaluaciones correspondientes, con el propósito de conocer el funcionamiento del Sistema y el logro de sus objetivos en todo el territorio nacional y, de manera especial, la trasmisión en tiempo real de la información relacionada con cada uno de los servicios.

**Artículo 50.-** Para el desarrollo de las funciones y procesos del Sistema, colaborarán con el Instituto:

- I. Los Poderes Ejecutivo, Legislativo y Judicial de la Federación y de las Entidades Federativas;
- II. Los Organismos Constitucionales Autónomos;
- III. Las autoridades municipales;
- IV. Las instituciones de educación, investigación y las agrupaciones y organizaciones sociales y privadas, y
- V. Los particulares, obligados en los términos de las disposiciones aplicables y/o los convenios que suscriban con el Instituto.

**Artículo 51.-** El Instituto, previo cumplimiento de las formalidades legales y administrativas correspondientes y el acuerdo favorable de su Junta de Gobierno, deberá brindar el apoyo que le soliciten:

- I. El Ejecutivo Federal y el Senado de la República en materia de tratados, convenios o acuerdos internacionales, cuando se establezcan derechos y obligaciones en materia de información y telecomunicaciones para la seguridad pública; y

- II. El Ejecutivo Federal, en caso de que se requiera información y comunicaciones para prevenir, y en su caso atender emergencias o catástrofes originas por desastres naturales.

## Sección II De la Administración del Instituto

**Artículo 52.-** El ejercicio de las funciones del Instituto, corresponde en el ámbito de sus respectivas competencias a la Junta de Gobierno, su director general y los servidores públicos en quien éste delegue facultades.

**Artículo 53.-** La Junta de Gobierno es el órgano superior de dirección del Instituto y estará integrada de la siguiente manera:

- I. El Secretario de Seguridad y Protección Ciudadana Federal, quien fungirá como presidente;
- II. Dos miembros designados por el Presidente de la República;
- III. Dos representantes nombrados por el Consejo Nacional de Seguridad Pública, que correspondan a entidades federativas;
- IV. Un representante de la Secretaría de Hacienda y Crédito Público;
- V. Un representante del Instituto Federal de Telecomunicaciones;
- VI. Un representante de la Universidad Nacional Autónoma de México, designado por su Rector;
- VII. Un representante del Instituto Politécnico Nacional designado por su director; y
- VIII. Un representante de las corporaciones de auxilio públicas y privadas, que deberá rotarse.

**Artículo 54.-** La designación de los miembros de la Junta de Gobierno deberá recaer en personas que reúnan los requisitos siguientes:

- I. Ser ciudadano mexicano y estar en pleno goce de sus derechos civiles y políticos;
- II. Ser profesional distinguido en materias relacionadas con la salud, la protección civil o la seguridad, así como haber ocupado, por lo menos durante cinco años, algún cargo de alto nivel en los sectores público o privado, o ser un académico de reconocido prestigio en las materias mencionadas, con excepción de su presidente; y

- III. No haber sido sentenciado por delitos dolosos, inhabilitado para ejercer el comercio o para desempeñar un empleo, cargo o comisión en el servicio público, ni removido de algún cargo del sector público o privado.

**Artículo 55.-** Son causas de remoción y/o suspensión de un miembro de la Junta de Gobierno:

- I. La incapacidad física o mental que impida el correcto ejercicio de sus funciones por más de tres meses;
- II. Utilizar en beneficio propio o de terceros, la información confidencial o de otra naturaleza de que disponga debido a su cargo, así como divulgar tal información en términos distintos a los autorizados por esta Ley;
- III. Someter a consideración de la Junta de Gobierno, a sabiendas, información falsa o alterada;
- IV. Participar en actos políticos, partidistas o religiosos con la representación del Instituto;
- V. No excusarse de participar en aquellas tomas de decisiones en las que sus intereses personales se encuentren en conflicto con los del Instituto;
- VI. Es causa de suspensión el encontrarse sujeto a un proceso penal; y
- VII. Dejar de reunir cualesquiera de los requisitos señalados en el artículo 54 anterior.

**Artículo 56.-** Compete a la Junta de Gobierno, dictaminar sobre la existencia de las causas de remoción señaladas en el artículo inmediato anterior, debiendo hacerlo a solicitud del director general del Instituto o de cuando menos dos de sus miembros. El dictamen se formulará según resolución de la mayoría de los miembros de la Junta de Gobierno, después de conceder el derecho de audiencia al afectado y sin que éste participe en la votación.

El dictamen, con la documentación que lo sustente incluida la argumentación por escrito que, en su caso, el afectado hubiere presentado, será enviado al Ejecutivo Federal para su resolución definitiva.

**Artículo 57.-** El Presidente de la Junta de Gobierno o el Director General del Instituto, podrán convocar a reuniones de la Junta de Gobierno a las que deberá asistir el Director General con voz, pero sin voto, auxiliado por un secretario de acuerdos.

Las sesiones de la Junta de Gobierno deberán celebrarse con la asistencia de por lo menos cinco de sus miembros. Si no concurriere el presidente, la sesión será presidida por el miembro con mayor antigüedad. En caso de que hubiere dos o más miembros con igual antigüedad, los miembros asistentes elegirán de entre ellos al que deba presidir la sesión.

Las resoluciones de la Junta de Gobierno requerirán, para su validez del voto aprobatorio de la mayoría de los miembros presentes, la persona que presida la sesión tendrá voto de calidad en caso de empate.

La Junta de Gobierno podrá acordar la asistencia de servidores públicos del Instituto a sus sesiones, para que le rindan directamente la información que les solicite, así como solicitar al Instituto realice invitaciones a otras instituciones.

A las sesiones de la Junta de Gobierno, podrán asistir los invitados que la propia Junta de Gobierno determine.

Las personas que asistan a las sesiones deberán guardar confidencialidad respecto de los asuntos que se traten en ellas, salvo autorización expresa de la Junta de Gobierno para hacer alguna comunicación.

Los cargos de los miembros de la Junta de Gobierno serán honoríficos.

**Artículo 58.-** El director general será designado por el Presidente de la República, y durará en su cargo seis años, que comenzarán el primero de enero del tercer año calendario del periodo correspondiente al presidente de la República.

**Artículo 59.-** En el caso de quedar vacante el puesto de director general, en tanto el Ejecutivo Federal nombre a quien lo sustituya, la Junta de Gobierno nombrará a un director interino.

**Artículo 60.-** El director general, para el desarrollo de sus funciones, se auxiliará de directores operativos y directores regionales, los que deberán estar considerados en el Reglamento Interno y en el Manual de Organización General del Instituto.

**Artículo 61.-** Las relaciones laborales de los trabajadores del Instituto, se sujetarán a lo dispuesto en el apartado B del artículo 123 de la Constitución Política de los Estados Unidos Mexicanos.

**Sección III**  
**De las Atribuciones de la Junta de Gobierno**

**Artículo 62.- Corresponden a la Junta de Gobierno las siguientes facultades:**

- I. Aprobar el Reglamento Interno y el Manual de Organización General del Instituto;**
- II. Proponer la información que debe ser de divulgación restringida o clasificada, como confidencial o reservada por motivos de seguridad nacional;**
- III. Aprobar el programa operativo anual y el proyecto de presupuesto anual;**
- IV. Aprobar el programa estratégico del Instituto, previa consulta necesaria al Consejo Consultivo Nacional;**
- V. Aprobar el establecimiento y cierre de los Centros de Supervisión y Control Regional, con base en la disponibilidad presupuestaria y previa consulta necesaria al Consejo Consultivo Nacional;**
- VI. Aprobar el nombramiento y remoción de los Directores Operativos y los Directores Regionales;**
- VII. Aprobar la imposición de sanciones administrativas por infracciones a la ley, en términos de las disposiciones legales aplicables;**
- VIII. Aprobar las políticas para la administración de los recursos humanos, financieros y materiales, en términos de las disposiciones aplicables;**
- IX. Aprobar las normas, políticas y especificaciones para la adquisición y determinación de la infraestructura tecnológica de los Complejos de Seguridad y de la Red Nacional de Telecomunicaciones; así como, de los proyectos específicos para dichos activos;**
- X. Resolver sobre otros asuntos relacionados con el contenido de esta ley, que cualquiera de sus miembros someta a su consideración;**

- XI. Someter a consideración del Consejo Consultivo Nacional del Sistema, los asuntos relacionados con el contenido de esta ley y cualquier otro que consideren pertinentes la Junta de Gobierno y el director general; y
- XII. Las demás que le asigne el CNSP.

#### **Sección IV De las Atribuciones del Director General**

**Artículo 63.-** Corresponde al director general del Instituto las siguientes atribuciones:

- I. Tener a su cargo la administración del Instituto, la representación legal de éste y el ejercicio de sus funciones;
- II. Someter a la consideración y, en su caso, aprobación de la Junta de Gobierno las políticas para la administración de recursos humanos, financieros y materiales del Instituto, de acuerdo con sus programas y objetivos;
- III. Aplicar y ejecutar los acuerdos tomados por la Junta de Gobierno;
- IV. Representar al Instituto ante el Consejo Consultivo Nacional;
- V. Someter para su aprobación ante la Junta de Gobierno, los expedientes para nombramiento y remoción de los directores operativos y directores regionales;
- VI. Aprobar la imposición de las sanciones administrativas por infracciones a la presente ley, que no requieran de la aprobación de la Junta de Gobierno, en términos de las disposiciones legales aplicables;
- VII. Delegar sus facultades en algún director operativo por un periodo no mayor a treinta días, para el despacho de los asuntos, salvo aquellas que se encuentran exclusivamente otorgadas y las de representación del Instituto.
- VIII. Someter a la consideración y, en su caso, aprobación de la Junta de Gobierno, el programa estratégico del Sistema y los demás instrumentos de planeación; el Programa operativo anual; el Reglamento interno; el Manual de Organización General del Instituto; el proyecto de presupuesto anual; el establecimiento y cierre de Centros de Supervisión y Control Regional del Instituto, así

- como el nombramiento de los Directores Operativos y de los Directores Regionales;
- IX. Ejecutar las políticas para la administración de los recursos humanos, financieros y materiales del Instituto;
  - X. Implementar las bases y lineamientos necesarios para las funciones de Conducción, Planeación y Evaluación; las de Supervisión y Control Regional; así como las de Investigación, Desarrollo e Innovación Científica y Tecnológica, emitiendo la normatividad general y específica para la operabilidad y gestión del Sistema;
  - XI. Planear las políticas públicas acordes al funcionamiento del Sistema, con la información y datos proporcionados por los Subsistemas de: Recopilación y Almacenamiento de Datos e Información; Procesamiento e Integración de las Bases de Datos; Explotación; Uso y Diseminación de la Información; e Interoperabilidad y Comunicaciones;
  - XII. Elaborar un informe anual de las actividades, estadísticas, programas y proyectos de los Subsistemas, así como de los logros alcanzados para su evaluación por la Junta de Gobierno; y
  - XIII. Las demás que le asigne la Junta de Gobierno del Instituto.

### **Capítulo III**

#### **De la Organización y Funcionamiento de las Unidades Administrativas del Instituto**

##### **Sección I**

#### **De la Estructura Orgánica y Funciones Esenciales y Directivas del Sistema**

**Artículo 64.-** Las funciones de conducción, planeación y evaluación estarán a cargo del director general, quien se auxiliará de dos directores operativos, uno para la planeación y evaluación y otro para la administración. Estas funciones tienen por objeto la gobernabilidad del Sistema, sujeto a normas y reglas técnicas uniformes en todo el territorio nacional. Estas funciones implican desarrollar, los siguientes procesos:

- I. Interacción con el entorno social nacional;
- II. Conducción y coordinación del Sistema;
- III. Regulación técnica y normatividad de los procesos, para lo cual autorizará la expedición de reglamentos, normas, lineamientos, procedimientos, instructivos, estándares y protocolos requeridos por los Subsistemas;

- IV. Planeación, prospectiva y estratégica;**
- V. Evaluación del Sistema y de sus Subsistemas; y**
- VI. Vigilancia del cumplimiento de las normas y lineamientos de los proyectos de diseño, contratación y operación de tecnologías de la información y comunicaciones, así como de la adquisición de infraestructura.**
- VII. Administración del Instituto: comprende la administración de personal; de adquisiciones de bienes y servicios; control de bienes y suministros; prestación de servicios generales; y todas las funciones de contabilidad y de control programático-presupuestal e inventarios de activos fijos.**

Así mismo, estarán a cargo del director general las funciones de supervisión y control regional para las cuales se auxiliará de un director regional para cada uno de los Centros de Dirección y Control Regional aprobados por la Junta de Gobierno.

Estas funciones tienen por objeto la armonización mediante la supervisión y control de los Complejos de Seguridad y de los nodos de la Red Nacional de Telecomunicaciones, para que se comporten como un todo integral, sujeto a reglas uniformes en todo el territorio nacional. Estas funciones implican desarrollar, al menos los siguientes procesos:

- I. Interacción con el entorno social regional;**
- II. Planeación, programación y presupuestación;**
- III. Supervisión, seguimiento, control y evaluación;**
- IV. Operación y capacitación;**
- V. Información regional; y**
- VI. Certificación de los Complejos de Seguridad, de conformidad con el Reglamento del Proceso de Certificación de los Complejos de Seguridad.**

**Artículo 65.- Los Centros de Supervisión y Control Regional, tendrán las siguientes funciones:**

- I. Identificar y pronosticar los sucesos sociales que afectan al Sistema, con el fin de introducir modificaciones en su estructura, para responder eficientemente a las nuevas condiciones del medio ambiente de la región que le corresponda;**
- II. Instrumentar las actividades de planeación, armonización, programación y presupuestación, de acuerdo con las normas dictadas por el director general del Instituto;**
- III. Supervisar y controlar a los Complejos de Seguridad e instalaciones de la Red Nacional de Telecomunicaciones, para lograr los objetivos del Sistema en la región que le corresponda;**

- IV. Dirigir y controlar el Complejo de Seguridad de respaldo para asegurar la estabilidad del Sistema en la región que le corresponda;
- V. Organizar y realizar los cursos de capacitación requeridos por el Centro de Supervisión y Control Regional y por los Complejos de Seguridad y demás instalaciones de su adscripción;
- VI. Instrumentalizar los sistemas informáticos y aplicaciones diseñados para los Centros de Supervisión y Control Regional, así como las aplicaciones de control de las instalaciones de la Red Nacional de Telecomunicaciones, en la región y en las entidades federativas que la comprendan; y
- VII. Implementar el proceso de certificación de los Complejos de Seguridad de conformidad con el Reglamento correspondiente.

**Artículo 66.-** Las funciones de Investigación, Desarrollo e Innovación Científica y Tecnológica, estarán a cargo del director general para las cuales se auxiliará de un director operativo.

Estas funciones tendrán por objeto realizar investigaciones para efecto de desarrollo e innovación científica y tecnológica en materia de Seguridad Pública, así como para regular todas las especificaciones en materia de TIC y comunicaciones.

Dichas funciones para su desarrollo deberán observar lo siguiente:

- I. Mantener un acervo actualizado de indicadores, protocolos y especificaciones de infraestructura física y de TIC de Seguridad Pública, en relación con la población y el medio ambiente;
- II. Asegurarse que todos los proyectos, cuando no sean de investigación básica, sean de investigación para los servicios que presta el Sistema a través del Instituto y los Complejos de Seguridad;
- III. Iniciar todas las investigaciones formulando un protocolo de conformidad con las normas internacionales aplicables;
- IV. Formular una bitácora con la información de los avances, hallazgos y resultados logrados en cada etapa;
- V. Para los efectos de sus investigaciones se ajustará a las normas y mejoras prácticas seguidas por las instituciones de educación superior;

- VI. Los resultados de las investigaciones, en su caso, serán materia de patente.**

**Artículo 67.- Las investigaciones se ajustarán a las disposiciones en materia de seguridad de la información y a las de diseminación de los resultados, cuando estén consideradas de Seguridad Nacional.**

## **Sección II De la Estructura Orgánica y Funcionamiento de los Subsistemas**

**Artículo 68.- Los Subsistemas de Información serán los comprendidos en los capítulos V al VII del Título Tercero de esta Ley y estarán a cargo, cada uno de ellos, de un director operativo auxiliado por el personal establecido en el Reglamento Interior.**

**Artículo 69.- Cada director operativo de los Subsistemas de Información tendrá las siguientes funciones generales:**

- I. Dirigir las actividades necesarias para alcanzar los objetivos y desarrollo de las funciones del Subsistema;**
- II. Instrumentar las actividades de planeación, armonización, programación y presupuestación, de acuerdo con las normas dictadas por el director general del Instituto;**
- III. Asegurar que los sistemas y aplicaciones se desarrollen conforme a las normas, lineamientos, estándares, protocolos y demás disposiciones establecidas para tal efecto;**
- IV. Vigilar que el uso y manejo de la infraestructura de TIC se ajuste a las normas de operación y conservación establecidas para tal efecto;**
- V. Asegurar que las infraestructuras de información esenciales y críticas se encuentren identificadas y clasificadas para la protección y seguridad de la información;**
- VI. Vigilar y asegurar que toda la información se ajuste a las normas de seguridad de la información a que se refiere el MAAGTIC;**
- VII. Vigilar y asegurar que la información esencial y crítica se maneje con apego a lo establecido en el artículo 34 de esta Ley, para los efectos de su diseminación;**
- VIII. Asegurar que todos lineamientos, normas y demás disposiciones en relación al Sistema de Información y cualquier cambio que se**

establezca al respecto, sea del conocimiento del personal de los Subsistemas y de los Complejos de Seguridad, así como los destinatarios de la información, de conformidad con lo señalado en el artículo 34 de esta Ley;

- IX. Observar respecto de los componentes de las bases de datos, locales y nacionales, lo siguiente:
  - a) Contar con el inventario institucional de bases de datos en las que se identifique cuales tienen interacción con otras bases de datos;
  - b) Impulsar su integración e instancias o esquemas para los diversos aplicativos de cómputo, de manera que sean eficientes los recursos con que cuenten los servidores; y
  - c) Salvaguardar los derechos de la propiedad intelectual, portabilidad y recuperación de los datos generados y procesados de acuerdo con el ciclo de vida de la información, incluyendo el borrado seguro.
- X. Organizar y realizar los cursos de capacitación requeridos por el personal del Subsistema, y de los Complejos de Seguridad; y
- XI. Las demás que resulten de esta Ley y de otras disposiciones legales aplicables.

**Artículo 70.-** El Subsistema de Interoperabilidad y Comunicaciones será el comprendido en el Capítulo VIII del Título Tercero de esta Ley, y estará a cargo de un director operativo auxiliado por el personal establecido en el Reglamento Interior.

**Artículo 71.-** El director operativo del Subsistema de Interoperabilidad y Comunicaciones tendrá las siguientes funciones generales:

- I. Dirigir las actividades necesarias para alcanzar los objetivos y desarrollo de las funciones del Subsistema;
- II. Instrumentar las actividades de planeación, armonización, programación y presupuestación, de acuerdo con las normas dictadas por el Director General del Instituto;
- III. Asegurar que los sistemas de comunicaciones se desarrollen conforme a las normas, lineamientos, estándares, protocolos y demás disposiciones establecidas para tal efecto;

- IV. Vigilar que el uso y manejo de la infraestructura activa y pasiva de la Red Nacional de Telecomunicaciones se ajuste a las normas de operación y conservación establecidas para tal efecto;**
- V. Asegurar que todos lineamientos, normas y demás disposiciones en relación al Subsistema de Interoperabilidad y Comunicaciones y cualquier cambio que se dé al respecto, sea del conocimiento del personal: del Subsistema; de los Complejos de Seguridad; y de la Red Nacional de Telecomunicaciones;**
- VI. Con respecto a sistemas de comunicaciones unificadas de telefonía y video, deberá observarse lo siguiente:**
  - a) Establecer interconexión de sistemas de telefonía entre instituciones, que disminuya costos e incremente la seguridad de las conversaciones, mediante la implementación de sistemas de seguridad de frontera específicos para comunicaciones de voz y video y se asegure el soporte de transcodificación de señalización entre diferentes formatos de comunicación;**
  - b) Utilizar tecnologías de mensajería instantánea, presencia y movilidad, a fin de incrementar la productividad de los usuarios y un mayor uso de estas, teniendo en consideración la seguridad de la información;**
  - c) Privilegiar el uso de teléfonos de bajo consumo de energía; y**
  - d) Utilizar tecnologías de gestión y monitoreo a fin de facilitar la implementación, operación y planeación de la capacidad instalada de telefonía y video.**
- VII. Organizar y realizar los cursos de capacitación requeridos por el personal del Subsistema; los Complejos de Seguridad; y en especial, de la Red Nacional de Telecomunicaciones; y**
- VIII. Las demás que resulten de esta Ley y de otras disposiciones legales aplicables.**

### **Sección III**

#### **De la Organización y Funciones de los Complejos de Seguridad**

**Artículo 72.-El director del órgano local descentralizado de la administración pública de la Entidad Federativa de los Complejos de Seguridad tendrá bajo su responsabilidad la regulación y normatividad de la prestación de los servicios y operación de dichos Complejos, tanto en sus funciones de información como de comunicaciones.**

**Artículo 73.-** La coordinación, supervisión y control de los Complejos de Seguridad estará a cargo de los Centros de Supervisión y Control Regional a que se refiere el artículo 65 de esta Ley.

**Artículo 74.-** Los Complejos de Seguridad desarrollarán los siguientes procesos:

- I. Prestación de los servicios públicos a que se refiere el artículo 13 de esta Ley;
- II. Los relativos a la información a que se refieren los subsistemas señalados en los capítulos V a VII del Título Tercero de esta Ley, dentro de su ámbito de influencia; y
- III. Procesos de comunicaciones del subsistema, regulado conforme al capítulo VIII del Título Tercero de esta Ley, dentro de su ámbito de influencia.

**Artículo 75.-** Los Complejos de Seguridad para el desarrollo de sus funciones contarán con una estructura de personal para atender las actividades relacionadas con sus procesos y administración.

**Artículo 76.-** La operación de los Complejos de Seguridad comprenderá, al menos, las siguientes funciones:

- I. Atender las instrucciones y formular los reportes regulares y emergentes del órgano descentralizado de la Entidad Federativa correspondiente de la dirección y operación de los Complejos de Seguridad;
- II. Atender y prestar los servicios públicos que les corresponde, de conformidad con los principios a que se refiere el artículo 12 de esta Ley;
- III. Desarrollar sus funciones, en lo conducente, y en especial cumplir con los procesos de:
  - a) Certificación que comprende el diagnóstico de los activos de TIC y sus correcciones y ajustes; y
  - b) Refrendo trianual de la certificación que comprende la auditoría de los procesos de adquisición y funcionamiento, y la revisión de los activos de TIC.

De conformidad con el Reglamento del Proceso de Certificación de los Complejos de Seguridad.

- IV. Desarrollar conforme a la normatividad los procesos relativos a la información prescritos por los subsistemas, dentro de su ámbito de aplicación;**
- V. Desarrollar conforme a la normatividad los procesos relativos a las comunicaciones prescritos por el subsistema, dentro de su ámbito de aplicación;**
- VI. Conservar y proteger las bases de datos de la seguridad pública que generen sus procesos;**
- VII. Conservar y proteger las bases de datos de información esencial y críticas generadas por sus procesos;**
- VIII. Operar, dentro de su ámbito de aplicación todas las actividades relacionadas con la Red Nacional de Telecomunicaciones;**
- IX. Llevar a cabo la recolección de datos que le sean proporcionados en los términos de esta Ley, por la Fiscalía autónoma de la Entidad Federativa y de la Guardia Nacional relacionados, con su ámbito territorial;**
- X. Realizar todas las actividades relacionadas con la seguridad de la información, en los términos de lo dispuesto en esta Ley;**
- XI. Llevar a cabo, con oportunidad y suficiencia, la transferencia de datos e información al CDCS para la integración de las Bases de Datos Nacionales;**
- XII. Desarrollar todas las actividades encaminadas a la conservación de las infraestructuras de TIC, activas y pasivas de comunicaciones y, en particular con las relacionadas con la información esencial y crítica, en los términos de las disposiciones legales aplicables; y**
- XIII. Las demás que resulten de esta ley y de otras disposiciones legales aplicables.**

#### **Capítulo IV Del Patrimonio del Instituto**

**Artículo 77.- El patrimonio del Instituto estará integrado por:**

- I. Los bienes inmuebles y muebles que la Federación le transfiera y que han estado asignados al Centro Nacional de Información del**

**Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y del Centro Nacional de Información Plataforma México, ambos de la Secretaría de Seguridad y Protección Ciudadana;**

- II. Los bienes inmuebles y muebles que adquiera para el cumplimiento de su objeto, incluyendo los que la Federación halla destinado para tal fin o para su uso exclusivo, así como los que le transfieran las Entidades Federativas y los municipios;**
- III. Las aportaciones en dinero o en especie que los tres Órdenes de Gobierno realicen a su favor;**
- IV. Los recursos que anualmente apruebe para el Instituto la Cámara de Diputados del Congreso de la Unión, en el Presupuesto de Egresos de la Federación; y**
- V. Las donaciones que reciba para el cumplimiento de su objeto y los ingresos que obtenga por cualquier otro concepto.**

**Artículo 78.- De la distribución de responsabilidades patrimoniales y presupuestales:**

- I. La Federación tendrá a su cargo la asignación de los recursos financieros, de inversión y materiales para la instalación, ampliación y funcionamiento de los servicios públicos bajo su responsabilidad, incluidos los que prestan los Centros de Supervisión y Control Regional y los Complejos de Seguridad de respaldo;**
- II. Los recursos del Instituto serán financiados con:**
  - a) Recursos presupuestales asignados al Instituto;**
  - b) Recursos transferidos de otras dependencias y entidades;**
  - c) Los que el Consejo Nacional de Seguridad Pública transfiera al Instituto, de los Fondos de Ayuda Federal para la Seguridad Pública;**
- III. Corresponderá a las entidades federativas y los municipios, aportar los terrenos y en su caso las edificaciones para la creación de los Centros de Supervisión y Control Regional y las instalaciones que se destinen a la Red Nacional de Telecomunicaciones, por acuerdo del**

**Consejo Nacional de Seguridad Pública, previa solicitud aprobada por su Junta de Gobierno.**

**Artículo 79.- El Instituto ejercerá su presupuesto, observando lo dispuesto en la Ley Federal de Presupuesto y Responsabilidad Hacendaria, sujetándose a lo siguiente:**

- I. Aprobará su proyecto de presupuesto y lo enviará a la Secretaría de Hacienda y Crédito Público, para su integración al proyecto de Presupuesto de Egresos de la Federación;**
- II. Las adecuaciones a su presupuesto no requerirán la autorización de la Secretaría de Hacienda y Crédito Público, siempre y cuando no rebasen el techo global de su presupuesto aprobado;**
- III. Realizará sus pagos a través de su Tesorería; y**
- IV. Llevará la contabilidad y elaborará sus informes, conforme a lo previsto en la Ley Federal de Presupuesto y Responsabilidad Hacendaria.**

**Artículo 80.- Los servicios que preste el Instituto serán gratuitos para la población en general.**

## **Capítulo V De la Información**

**Artículo 81.- Los datos que proporcionen, las instancias y sujetos del Sistema y todas las personas físicas o morales, usuarios de los servicios del Sistema, al Instituto y en especial a los Complejos de Seguridad en términos de la presente Ley, serán estrictamente confidenciales y en ninguna circunstancia podrán utilizarse para otro fin distinto de éste, en términos de las disposiciones legales aplicables.**

**El Instituto no deberá proporcionar a persona alguna, los datos a que se refiere este artículo para ningún fin, con excepción de aquellos que solicite y autorice la autoridad competente.**

**Artículo 82.- Los usuarios del Sistema podrán denunciar ante las autoridades administrativas y judiciales, todo hecho o circunstancia que derive del mismo, en los que se hubiesen desconocido los principios de confidencialidad y reserva a que se refiere esta ley.**

**Artículo 83.- El Instituto y los Complejos de Seguridad, tomarán las medidas pertinentes para asegurar la transmisión en línea y en tiempo real al CDCS, de**

los registros digitales y de los datos e información que deban integrarse a las Bases de Datos Nacionales.

De igual manera, lo harán para las correcciones y modificaciones que se hagan a dichos registros, conforme al protocolo correspondiente.

**Artículo 84.-** Las instancias y sujetos del Sistema a que se refiere el artículo 15 de esta Ley están obligados a proporcionar y en su caso compartir la información que les requiera el Instituto sobre Seguridad Nacional de que dispongan u obren en sus bases de datos.

**Artículo 85.-** Las instancias y sujetos a que se refieren las fracciones IV a VII del artículo 15 de esta Ley, deberán realizar los trabajos para lograr la compatibilidad de los servicios de telecomunicaciones, con las Bases de Datos Nacionales, de conformidad con el protocolo respectivo.

**Artículo 86.-** El Instituto participará en la elaboración de la EDN en los aspectos que le requiera la Coordinación de dicha estrategia y desarrollará las TIC en materia de seguridad nacional, compartiéndolas cuando así sea viable con entes de la APF.

**Artículo 87.-** El Instituto coordinará acciones y, en su caso suscribirá convenios de colaboración con órganos constitucionales autónomos, gobiernos de las entidades federativas y municipios, poderes legislativo y judicial de la federación y de las entidades federativas, instituciones privadas, públicas, nacionales e internacionales y con la sociedad en general, cuya finalidad sea la de impulsar el uso y aprovechamiento de las TIC en materia de seguridad pública.

**Artículo 88.-** El Instituto recibirá y emitirá recomendaciones de y con los entes de la APF, respecto de las mejores prácticas, susceptibles de desarrollar e implementar a través de proyectos e iniciativas estratégicas en materia de TIC y seguridad de la información.

## **Capítulo VI**

### **De la Profesionalización del Personal del Instituto**

#### **Sección I**

#### **Del Ingreso del personal**

**Artículo 89.-** La Junta de Gobierno aprobará el perfil profesional del personal del Instituto, observando en todo momento la no discriminación y la igualdad de oportunidades.

**Artículo 90.-** En la selección del personal que integrará el Instituto, en todo momento y sin distinción, deberá apegarse al perfil profesional asociado a cada puesto.

**Artículo 91.-** El personal que integrará el Instituto y los Complejos de Seguridad, deberá aprobar las evaluaciones de acuerdo con la normatividad establecida para la seguridad pública, en materia de: médico-toxicológica, psicológica, poligráfica, socioeconómica y de control de confianza; además de contar con la certificación de capacidades.

**Artículo 92.-** La certificación de capacidades, deberá determinar las aptitudes del nivel de dominio de los conocimientos y habilidades requeridas para el puesto a desempeñar, y contará para fines de ingreso, permanencia o de desarrollo profesional.

## **Sección II**

### **De la Permanencia y Capacitación del personal**

**Artículo 93.-** La Junta de Gobierno aprobará los criterios para la regulación de la permanencia, capacitación y profesionalización del personal que integra el Instituto.

**Artículo 94.-** La permanencia del personal estará en función de los mecanismos de medición cualitativos y cuantitativos que se establezcan para el cumplimiento de las funciones y metas individuales y del perfil determinado para el puesto que ocupan.

**Artículo 95.-** Se consideran como parte de los requisitos de permanencia del personal, los resultados que arrojen los procesos de evaluación de confianza. El personal no adquiere permanencia en su cargo por el solo hecho de cumplir con los requisitos de ingreso y por el transcurso de tiempo laborado.

**Artículo 96.-** Los resultados de las evaluaciones del personal no tienen ninguna relación con la imposición de sanciones, responsabilidad civil o administrativa alguna.

**Artículo 97.-** La capacitación al personal del Instituto será permanente y tendrá por objeto lograr una mejor y eficaz prestación del servicio; incluye al personal de nuevo ingreso y al personal que ya se encuentra laborando.

**Artículo 98.-** Los Complejos de Seguridad se sujetarán a la normatividad que establezca el Instituto en materia de capacitación. Ésta última, siempre será proporcionada por el Instituto y cuando esto no fuere posible, éste autorizará los contenidos e impartición de los cursos correspondientes.

**Artículo 99.-** La capacitación del personal del Instituto y de los Complejos de Seguridad, se ajustará periódicamente en respuesta a la adaptación de la tecnología para conservar su conocimiento, aptitudes, habilidades, y conciencia sobre los sistemas y controles internos.

**Artículo 100.-** Es responsabilidad del Instituto, a través de los Centros de Supervisión y Control Regional y de los Complejos de Seguridad, identificar las necesidades de desarrollo y capacitación de su personal para las tecnologías de la información y comunicaciones que se utilizan en las áreas correspondientes.

**Artículo 101.-** Los Programas de Capacitación deberán ser aprobados por el director general previa opinión del Consejo Consultivo Nacional y contemplar al menos los siguientes conceptos:

- I. Necesidades estratégicas de capacitación;
- II. Necesidades de capacitación específica;
- III. Temas de capacitación;
- IV. Compromisos de capacitación;
- V. Métodos para utilizar en la capacitación;
- VI. Requerimientos para materiales de capacitación;
- VII. Recursos necesarios para la capacitación (herramientas, instalaciones, personal);
- VIII. Diagrama de tiempos para la capacitación; y
- IX. Resultados esperados.

**Artículo 102.-** La capacitación puede ser proporcionada por especialistas técnicos en TIC del Instituto o por un proveedor externo, tomando en consideración en todo momento el costo-beneficio de quien facilite la capacitación.

## **TITULO QUINTO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES**

### **Capítulo I**

#### **De la Formulación de Proyectos de Infraestructura Física, de Información y de Comunicaciones**

**Artículo 103.-** Este capítulo tiene por objeto regular la creación, modificación y adaptación de la infraestructura física y/o de equipamiento (hardware) y de programas informáticos (software); y aplicaciones de TIC. Asimismo, incluye infraestructura activa y pasiva de comunicaciones.

Las reglas comprenden elementos de TIC de servicios, existentes o nuevos, y otros activos del Sistema. También a la solución de problemáticas sobre carencias, deficiencias y/o insuficiencias, preexistentes, identificadas y diagnosticadas en términos mensurables de costo-beneficio a la población.

**Artículo 104.-** La regulación a que se refiere este título se fundamenta en las reglas que resulten aplicables en materia de seguridad pública, por las

disposiciones a que se refiere la EDN en materia de TIC y en la de seguridad de la información; la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; y demás disposiciones que resulten aplicables.

### Sección I

#### Reglas Generales para la Formulación de Proyectos Generales

**Artículo 105.-** La creación, modificación y adaptación a que se refiere el artículo 103 de esta Ley, deberá llevarse a cabo formulando un proyecto general, que comprenda los procesos de: programas arquitectónicos y de TIC para cada proyecto; y los proyectos ejecutivos que podrán referirse, tanto a la infraestructura física, como a la de TIC (hardware) y los programas informáticos (software).

Los proyectos generales deberán, además, referirse a los siguientes procedimientos: equipamiento y programación informática, y adquisiciones. Estos procesos comprenden a los subprocesos de: instalación, capacitación, implementación, operación y conservación, y mantenimiento.

### Sección II

#### De los Indicadores de Programación y Evaluación

**Artículo 106.-** Los proyectos a que hace referencia la sección I de este capítulo deberán formularse con apego a los indicadores de programación de equipamiento de los servicios, que son los estándares mínimos de equipamiento de los distintos componentes que requiere cada uno de los servicios que presta un Complejo de Seguridad.

Estos relacionan una variable, que es la cantidad de unidades de equipos por cada unidad de servicio, en relación con una cantidad de población o de características de cada equipo. Estos estándares permiten la programación de equipos requeridos por los Complejos de Seguridad para una población determinada o servicios a prestar. Los principales estándares mínimos de equipamiento para un Complejo de Seguridad o instalación análoga son:

**Estándares de equipamiento de servicios**

Servicio	Clases de Unidades de Equipamiento	Cantidad de Unidades	Unidades de Medida relacionadas
1. Llamadas de emergencia (911)	Estaciones de Atención	1	103.7 miles de habitantes
2. Llamadas de denuncia anónima (089)	Estaciones de Atención	1	

<b>3. Videovigilancia</b>	<b>Resolución del medio de captación (cámara) Dimensión física de la imagen en el medio de proyección (monitor)</b>	<b>Megapíxeles en el medio de captación Centímetros en el medio de proyección</b>	<b>2 Megapíxeles o equivalente en el medio de captación 5 x 7 centímetros por imagen en un esquema de imágenes múltiples (mosaico)</b>
<b>4. Sistema de alarma Aviso de pánico</b>	<b>Indicadores en el panel de control o medio de proyección</b>	<b>Número de indicadores</b>	<b>64 indicadores por panel de control o medio de proyección</b>
<b>5. Rastreo vehicular</b>	<b>Unidades de rastreo</b>	<b>Unidades por tipo de cobertura</b>	<b>20 unidades de rastreo en cobertura de zona 10 unidades de rastreo en cobertura dedicada</b>

**Artículo 107.-** Los indicadores de evaluación, son indicadores de desempeño que permiten establecer parámetros de avance en el cumplimiento de los objetivos y metas. Los principales mínimos de desempeño están dados por los estándares para este tipo de indicadores, para cada uno de los siguientes servicios.

**I. Estándares de desempeño del Servicio de Atención de Llamadas de Emergencia:**

<b>Descripción</b>	<b>Estándar</b>
<b>1. Tiempo de respuesta de llamada</b>	<b>NO &gt; 20 Segundos</b>
<b>2. Recepción de la llamada</b>	<b>NO &gt; 90 Segundos</b>
<b>3. Despacho de la llamada</b>	<b>NO &gt; 120 Segundos</b>
<b>4. Atención de la emergencia</b>	<b>NO &gt; 9 Minutos</b>

**II. Estándares de desempeño para los servicios de: video vigilancia o alarmas o botones de pánico o GPS:**

<b>Descripción</b>	<b>Estándar</b>
<b>1. Efectividad de Captación Global (ECG)</b>	<b>Lo más próximo al 100%</b>
<b>2. Efectividad de Captación de Campo (ECC)</b>	<b>Lo más próximo al 100%</b>
<b>3. Efectividad de Detección de Eventos (EDE)</b>	<b>Lo más próximo al 100%</b>

**Artículo 108.-** Los principales indicadores de desempeño para cada uno de los siguientes servicios son:

**I. Servicio de Atención de Llamadas de Emergencia**

<b>Indicador</b>
<b>1. Promedio de tiempo de la recepción de la llamada de emergencia.</b>
<b>2. Porcentaje de llamadas fuera del tiempo establecido.</b>
<b>3. Promedio de tiempo en el despacho de la llamada.</b>
<b>4. Promedio de tiempo en la atención de la emergencia.</b>
<b>5. Porcentaje de llamadas colgadas.</b>
<b>6. Porcentaje de llamadas en cola.</b>
<b>7. Porcentaje de incidentes tipificados correctamente.</b>
<b>8. Porcentaje de incidentes despachados.</b>
<b>9. Porcentaje de incidentes atendidos.</b>
<b>10. Porcentaje de incidentes atendidos en el tiempo establecido.</b>
<b>11. Porcentaje de llamadas que cumplen con los procesos.</b>
<b>12. Porcentaje de incidentes despachados que no son emergencias.</b>
<b>13. Porcentaje de incidente con folio no cerrado.</b>

**II. Indicadores de desempeño de los servicios de: video vigilancia o alarmas o botones de pánico o GPS:**

<b>Indicador</b>
<b>1. Porcentaje de eventos captados del total de eventos ocurridos en el área.</b>
<b>2. Porcentaje de eventos distinguidos del total de eventos captados.</b>
<b>3. Porcentaje de eventos detectados susceptibles de emitir un alertamiento, del total de eventos captados.</b>

**Sección III  
De la Programación**

**Artículo 109.-** Los proyectos de infraestructura física, de equipamiento y programas informáticos de TIC, deberán respaldarse, en primer término, con el correspondiente programa arquitectónico y, en segundo término, con el programa de equipamiento y programas informáticos requeridos.

Todo proyecto general deberá fundamentarse en la programación de los servicios requeridos para la atención de la población comprendida en el ámbito espacial del Complejo de Seguridad o Centro de Supervisión y Control Regional, con base en los indicadores de servicio a que se refieren los artículos 106 a 108 de esta Ley.

**Artículo 110.-** La programación señalada en el artículo anterior deberá comprender también una perspectiva de los servicios para los siguientes cinco años, con indicadores de desempeño que permitan evaluar el avance cuantitativo y cualitativo, de los servicios de cada Complejo de Seguridad.

**Artículo 111.-** El programa arquitectónico realizado con base en la población del área de influencia, deberá comprender al menos, las áreas para los centros

de: monitoreo del sistema de video vigilancia; atención de llamadas de emergencia; llamadas de denuncia anónima; y recepción de tecnologías emergentes.

Así también, comprenderá las áreas para las instalaciones: hidráulica, sanitaria, eléctrica e iluminación y las requeridas para: la energía eléctrica y subestación, el sistema de tierras, las celdas solares, el aire acondicionado y confort, el sistema contra incendio y el circuito cerrado de televisión, y todas las áreas de circulación y de servicios adjetivos de apoyo a la operación.

#### Sección IV De los Proyectos Ejecutivos

**Artículo 112.-** Los proyectos ejecutivos de infraestructura física, deberán formularse con base en los resultados de los programas arquitectónicos y comprenderán las memorias de cálculo, planos a detalle, costos y precios unitarios, validación de perito, certificación de instalación y especificaciones técnicas de cada ingeniería; así como también debe contener los estudios preliminares de levantamiento topográfico, estudio de mecánica de suelos, el costo total estimado de la ejecución de la obra y los documentos que se requieren para las gestión del Estudio de Impacto Ambiental y los permisos y licencias.

Asimismo, el proyecto ejecutivo debe contener los requisitos mínimos necesarios para el proceso licitatorio y posteriormente la implementación y ejecución. El proyecto ejecutivo considerara los servicios adjetivos requeridos por el Complejo de Seguridad, como es el resguardo, preservación y administración de la información y datos obtenidos del sistema de video vigilancia y de las tecnologías emergentes.

También deberán contener todas las especificaciones a que se refiere el apartado 5.11 infraestructura física del "Manual Técnico de la Norma para homologar características y TICs de los Centros de Control, Comando, Cómputo y Comunicaciones".

**Artículo 113.-** Los proyectos ejecutivos de TIC deberán establecer el equipamiento (hardware) de las mismas a que se refiere el capítulo II y los programas informáticos (software) a que se refiere el capítulo III, ambos de este Título.

En especial todos los proyectos ejecutivos de TIC deberán considerar, además del presupuesto de costo de construcción y/o adquisición, la proyección presupuestal, tanto de la implementación, como de la operación y conservación durante la vigencia de su vida útil, calculado a valor presente.

Los presupuestos y costos referidos, deberán considerar obligatoriamente los siguientes instrumentos del Sistema: Convenios Marco en el caso de existir, el Padrón de Proveedores y los Precios de Referencia.

Asimismo, se deberán considerar las disposiciones siguientes y las de los artículos 114 al 116 de este ordenamiento:

- I. El uso del cómputo en la nube para el aprovechamiento de menores costos;
- II. Privilegiar la aplicación de Tecnologías verdes;
- III. Formular un anexo en el cual se registre el presupuesto estimado y de ser el caso, el presupuesto autorizado, para el ejercicio fiscal, así como las necesidades adicionales;
- IV. Identificar las características, específicas y estándares generales de los principales componentes del equipamiento y los programas informáticos;
- V. Instituir estrategias de interoperabilidad al interior del Instituto y con otras instituciones que sean necesarias, y que compartan datos que obren en su posesión;
- VI. Fundamentarse en su caso, en: Normas Oficiales Mexicanas, Normas Mexicanas y Normas Internacionales, en términos de Ley Federal sobre Metrología y Normalización;
- VII. Formular el análisis de riesgos, para identificar fuentes de vulnerabilidad;
- VIII. La transferencia, envío y recepción de datos, deberá realizarse sobre canales seguros en donde se favorezca el cifrado e integridad de datos críticos, confidenciales y sensibles, en lo que respecta a la Seguridad de la Información; y
- IX. Fijar especificaciones de diseño, codificación y seguridad de los programas informáticos (software).

**Artículo 114.-** Los proyectos ejecutivos deberán observar, respecto de las Redes de Comunicación lo siguiente:

- I. Establecer un dominio o segmento virtual en el uso compartido de Redes de Comunicación;
- II. Mecanismos estándar de cifrado de datos;
- III. Incluir mecanismos que soporten y habiliten servicios de multidifusión en redes privadas o locales, así como en redes de área amplia, para soportar envío de información y datos en video;
- IV. Proporcionar las medidas necesarias para el óptimo funcionamiento de los equipos que conforman la red de telepresencia, considerando al menos equipos de conmutación de datos, ruteadores, equipos ópticos e infraestructura pasiva con los que cuenten; y
- V. Considerar que los equipos de frontera soporten como mínimo la versión 4 y preferentemente se instale la última versión del protocolo de internet.

**Artículo 115.-** En el caso de los servicios de los Centros de Datos, los proyectos ejecutivos deberán observar lo siguiente:

- I.** Identificar la infraestructura del Centro de Datos con la que cuenta y la utilización de esta, así como el espacio físico, energía eléctrica, capacidad de procesamiento y almacenamiento;
- II.** Analizar el alojamiento de su infraestructura crítica en un Centro de Datos de otra área agrupada en su mismo sector;
- III.** Almacenar y administrar en el Centro de Datos que se encuentre en las instalaciones, los datos considerados de seguridad nacional y seguridad pública conforme a la normatividad aplicable;
- IV.** Mantener en la infraestructura de los Centros de Datos una arquitectura que permita portabilidad, de forma tal, que las aplicaciones de cómputo puedan migrar entre distintos Centros de Datos y sean interoperables. Dicha infraestructura deberá ser compatible con el uso de máquinas virtuales; y
- V.** Establecer en zonas de seguridad física y lógica, la infraestructura y administración de la seguridad de la información, considerando identidad, perfiles y privilegios, incluyendo en estas las necesarias para el personal involucrado, conforme a los controles de seguridad de la información.

**Artículo 116.-** En los proyectos ejecutivos de TIC se deberá observar, respecto de los sistemas de comunicaciones unificados de telefonía y video, lo siguiente:

- I.** Utilizar tecnología que soporte como mínimo la versión 4 del protocolo de internet y los mecanismos de cifrado estándar que resulten aplicables en las comunicaciones de voz y video, cifrado en señalización;
- II.** Utilizar marcación simplificada en un máximo de tres dígitos (911, 088, 089) o en su defecto de diez dígitos;
- III.** Establecer interconexión de sistemas de telefonía entre instituciones, mediante sistemas de seguridad de frontera específicos para comunicaciones de voz y video y se asegure el soporte de transcodificación de señalización, entre diferentes formatos de comunicación;
- IV.** Utilizar tecnologías de mensajería instantánea, presencia y movilidad; y

- V. Utilizar esquemas de consulta y acceso a directorio u otra base de datos normalizada para control de accesos y usuarios.

#### Sección V

#### De la Seguridad de la Información y de la considerada de Seguridad Nacional

**Artículo 117.-** Cada Centro de Datos del Instituto y de los Complejos de Seguridad, elaborarán su catálogo de infraestructuras de información esenciales y activos clave, e identificará en su caso, las que tengan el carácter de infraestructuras críticas de información, el cual deberá estar permanentemente actualizado con el fin de facilitar los controles para su protección.

**Artículo 118.-** Los Centros de Datos del Instituto y de los Complejos de Seguridad, desarrollarán un análisis de riesgos, que identifique, clasifique y priorice los mismos de acuerdo con su impacto en los procesos y servicios. Asimismo, previo al inicio de la puesta en operación de un aplicativo de cómputo, realizarán el análisis de vulnerabilidades correspondiente.

**Artículo 119.-** Los Centros de Datos del Instituto y de los Complejos de Seguridad, mantendrán los componentes de los programas informáticos y de seguridad de los dominios tecnológicos actualizados, para evitar vulnerabilidades, por lo que se implementarán, entre otros, elementos de seguridad de la información, los siguientes:

- I. Establecer directrices de seguridad de la información, mismas que podrán ser complementadas con base en mejores prácticas y estándares internacionales en la materia;
- II. Establecer controles de seguridad en los Activos de TIC, priorizando aquellos de mayor nivel de riesgo;
- III. Mantener evidencia auditable del proceso de borrado seguro;
- IV. Utilizar mecanismos de autenticación y cifrado de acuerdo con estándares internacionales, con un grado no menor a 256 bits para la protección de la comunicación inalámbrica;
- V. Utilizar redes abiertas únicamente al proporcionar servicios a la población, las cuales deberán estar separadas y aisladas de su red de datos; e
- VI. Implementar medidas y procedimientos para el respaldo de información.

**Artículo 120.-** El Instituto y los Complejos de Seguridad, a través de sus Centros de Datos, observará las disposiciones siguientes:

- I. La información relacionada con la seguridad nacional, generada o custodiada, que se pretenda diseminar, deberá identificarse previamente, en el nivel que corresponda de conformidad con lo establecido en el artículo 34 de esta Ley
- II. Asegurarse de que el destinatario de la información que se pretende diseminar tenga la necesidad de conocer de la misma, por ser el destinatario expreso de la información con motivo de las facultades conferidas por virtud de su empleo, cargo o comisión;
- III. Al diseminarse la información del nivel identificado, deberá asegurarse que aquella que se contenga en medios magnéticos, ópticos o electrónicos, cuente al menos con las medidas de protección siguientes:
  - a) Se incluya una carátula al inicio del documento, con la leyenda relativa al nivel de diseminación asignado, así como el nombre y cargo o código de seguridad del destinatario;
  - b) El documento electrónico deberá diseminarse en un formato de archivo que no permita su edición o manipulación y protegido de origen contra impresión o copiado no autorizado, parcial o total, de su contenido;
  - c) Se utilizarán mecanismos de cifrado de llave pública y privada, canales cifrados de comunicación y, cuando corresponda, de firma electrónica avanzada, que permitan la diseminación de la información únicamente al destinatario autorizado al que esté dirigida;
  - d) Comunicar a los destinatarios sobre la responsabilidad que éstos adquieren al recibir la información; y
  - f) Las demás medidas de protección que, de acuerdo con los riesgos y amenazas identificados, considere necesario adoptar.

## **Capítulo II** **Del Equipamiento de TIC (Hardware)**

### **Sección I**

**De la infraestructura de TI central, regional y de los Complejos de Seguridad**

**Artículo 121.-** El Sistema de Atención de Llamadas de Emergencia 9-1-1, deberá contar con la siguiente infraestructura de equipamiento: central telefónica; equipo de cómputo; y equipo telefónico. Este, deberá permitir comunicación con otros Complejos de Seguridad, con el Sistema de Videovigilancia y con el equipo telefónico de controles de acceso al equipo del operador. Todo el equipamiento del Sistema, deberá permitir el servicio de

las tecnologías emergentes. Las características mínimas de los equipos se detallarán en el Manual de Atención de Llamadas de Emergencia 9-1-1.

**Artículo 122.-** El Sistema de Video vigilancia para los Complejos de Seguridad, deberá contar con la siguiente infraestructura de equipamiento: equipo dedicado, conectado a la red de datos o equipo de cómputo con servidor o almacenamiento en disco; equipo telefónico; palanca de control para cámaras PTZ; y conjunto de pantallas agrupadas para visualizar una o varias imágenes en un área mayor. Las especificaciones técnicas de estos equipos se deben determinar en un Manual del Sistema de Video vigilancia para los Complejos de Seguridad.

**Artículo 123.-** El Sistema de Atención de Llamadas de Denuncia Anónima 089, deberá contar con la siguiente infraestructura de equipamiento: central telefónica; equipo de cómputo; equipo telefónico y controles de acceso al equipo del operador. La central telefónica constará de un conmutador y enrutadores que deberán ser de alto desempeño y con alta disponibilidad TIER III. Las especificaciones técnicas de estos equipos se deben determinar en un Manual del Sistema de Atención de Llamadas de Denuncia Anónima 089.

**Artículo 124.-** El equipamiento señalado en los artículos 121 a 123, deberá permitir la entrada de señales, voz, imágenes y datos a través de los sistemas operativos que provengan de: arcos lectores de reconocimiento de placas; cámaras móviles; aplicaciones móviles; sensores/alarmas de pánico y botones de emergencia; y drones.

**Artículo 125.-** El Sistema de Bases de Datos, deberá contar, según las necesidades de almacenamiento, con arquitectura de: servidores espejo, servidores escalables y servidores de alta demanda de cómputo. Los servidores deberán contar con discos duros superiores a los 180 IOPS, que garanticen en todos los casos redundancia e integridad de datos, siendo su capacidad de uso no mayor a 80%. Según la arquitectura de almacenamiento, los discos deberán ser compatibles con los sistemas especificados en el Manual correspondiente. La arquitectura de alta demanda de cómputo deberá contar con canales de alta velocidad.

**Artículo 126.-** El Sistema de Circuito Cerrado de Televisión (CCTV), deberá contar con la siguiente infraestructura de equipamiento: del mismo tipo de equipamiento para el Sistema de Video vigilancia, dimensionado en función del número de cámaras que se hayan definido para este circuito. Las cámaras serán de distintas especificaciones técnicas a la del Sistema de Video vigilancia, debiendo quedar establecidas en el Manual del Circuito Cerrado de Televisión.

**Sección II**  
**De las Infraestructura de Redes de Comunicación Locales, Estatales y Nacional**

**Artículo 127.-** La Red local (red interna) de los Complejos de Seguridad tiene por objeto garantizar la adecuada operación de la infraestructura de equipos y servicios de voz, video y datos. Deberá contar al menos con: cableado estructurado para equipos de telecomunicaciones; cableado horizontal; cableado principal; cableado de cobre; y canalización del cableado estructurado.

**Artículo 128.-** Las características de los cables y demás elementos de instalación, las normas para la instalación de la Red y los espacios y características de sus construcciones se determinarán en el Manual de la Red Local de los Complejos de Seguridad.

**Artículo 129.-** La Red local de los Complejos de Seguridad deberá contar con los siguientes equipos mínimos: conmutadores de datos, enrutadores y equipo de seguridad para la Red LAN. Las características mínimas de los conmutadores deben contar con puertos 10/100/1000 de tecnología ethernet e interfaces con conectores para módulos de fibra óptica.

**Artículo 130.-** La Red Estatal de Radiocomunicación, para sus servicios de voz y datos, contará con al menos el equipo básico para cada uno de los siguientes subsistemas:

- I. De conmutación: conmutadores, sistemas de geolocalización y sistema de grabación, entre otros;
- II. De Radio: estaciones base, terminales de radio, sistema de interoperabilidad de comunicaciones, puerto de enlace de radiocomunicación y donador de radio;
- III. De servidores: al menos uno para la base datos de la red; otro para los aplicativos para la configuración y gestión de la red y otro para los informes y alarmas.

**Artículo 131.-** La Red Nacional de Telecomunicaciones es un sistema integrado en los términos señalados en el artículo 3 de la Ley Federal de Telecomunicaciones y Radiodifusión, que tiene como finalidad la emisión, trasmisión o recepción de signos, señales, datos, escritos, imagen, voz, sonidos o información de cualquier naturaleza, en las bandas del espectro radioeléctrico señaladas en el Programa Anual de Usos y Aprovechamiento de Bandas de Frecuencia, así como en los recursos orbitales para servicios de seguridad pública.

**Capítulo III**  
**De los Programas Informáticos (Software) para las Facilidades Funcionales de TIC**

**Artículo 132.- El Sistema de Gestión de Incidentes (CAD, por sus siglas en inglés) es un sistema que debe comprender los aplicativos para:**

- I. Captura de la información en el momento de atender un llamado de emergencia, cuyos datos mínimos deben ser: geolocalización del lugar desde donde se reporta la emergencia; datos generales del ciudadano que reporta la emergencia; número telefónico desde donde se reporta la emergencia y tipo de emergencia;**
- II. Permitir ser el medio por el cual el sistema de video vigilancia y el área de operadores se deben comunicar;**
- III. Transferir la llamada al área del despacho de las emergencias a los servicios de auxilio;**
- IV. Asegurar que los eventos sean registrados en la base de datos correspondiente; y**
- V. La interconexión de los sistemas a través de la Red LAN.**

**Este sistema comprende los protocolos, lineamientos y especificaciones contenidos en el Manual del Sistema CAD.**

**Artículo 133.- La Red LAN está integrada por el conjunto de aplicativos con sus respectivos programas que permiten soportar las comunicaciones y mandatos analógicos de la video vigilancia, el sistema 9-1-1, el sistema 089, el circuito cerrado de televisión y su interconexión con otras redes.**

**El sistema de la Red LAN debe permitir la interoperabilidad interna con los dispositivos de comunicaciones; dispositivos de seguridad; cuartos de telecomunicaciones y equipos; alta disponibilidad en servidores y almacenamiento; y alta disponibilidad en equipo de comunicaciones. Asimismo, debe permitir la interoperabilidad a través de la interfaz de comunicaciones con la Red Estatal de Transporte de Datos y la Red Nacional de Telecomunicaciones, ambas para la seguridad pública.**

**Artículo 134.- Los CDCOS, los CDCR y el CDCS, deberán contar con los aplicativos y programas informáticos (software) requeridos para el debido funcionamiento de los servicios, sistemas operativos y equipos informáticos (hardware) que deberán estar debidamente aprobados por los responsables autorizados del Instituto.**

**Artículo 135.- Las áreas técnicas de cualquier instancia del Instituto podrán diseñar y formular los correspondientes proyectos de TIC, o proponer la**

adquisición de sistemas y aplicaciones para el debido funcionamiento de los servicios que proporciona el Instituto, los que después de ser autorizados por las instancias responsables se implementarán conforme a las disposiciones de esta Ley.

#### **Capítulo IV De los Procesos de Adquisición**

**Artículo 136.-** El Instituto, para la contratación de infraestructura física y de TIC en sus modalidades de adquisición, arrendamiento y servicios, previamente deberá haber formulado los proyectos Ejecutivo a que se refieren los artículos 112 y 113 de esta Ley, además de sujetarse a las disposiciones que se establecen en la Ley de Obras Públicas y Servicios Relacionados con las Mismas y en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, sus Reglamentos correspondientes y demás disposiciones aplicables en la materia. Asimismo, deberá observar lo siguiente:

- I. Para la contratación de servicios, se establecerá en la convocatoria a la licitación pública, en la invitación a cuando menos tres personas, en las solicitudes de cotización, o en el contrato que se celebre, según corresponda, la obligación de presentar, además de los precios unitarios del servicio, un desglose de los componentes técnicos que integren el servicio a prestar, de acuerdo con la normatividad aplicable;
- II. En los procesos de contratación de arrendamiento con opción de compra (arrendamiento financiero) de TIC, deberá establecerse cláusula específica sobre el acceso, control y posesión en condiciones de confidencialidad y privacidad de infraestructura y contenidos de información esenciales y críticos, asegurando mediante cláusula, también específica, que los contenidos de información en los equipos son propiedad reservada con exclusividad para el Estado Mexicano, por razones de seguridad pública y nacional.  
  
En el caso de terminación del contrato con devolución de los equipos, antes de que se realice ésta, deberá establecerse un plazo para la misma, que permita al Estado Mexicano rescatar de dichos equipos la información;
- III. Contratar bienes o servicios que respeten los derechos de propiedad intelectual de terceros;
- IV. La DOTIC registrará en su proyecto ejecutivo, su estudio de factibilidad y verificará que se le haya anexado lo siguiente:

- a) El estudio de costos y presupuestos basados en: los Convenios Marco en su caso; el Padrón de Proveedores y los Precios de Referencia, conforme a lo dispuesto al artículo 113 de esta Ley;
- b) El resultado de la investigación de mercado;
- c) El estudio de costo beneficio;
- d) El pronunciamiento sobre la existencia o inexistencia de un ente público que esté en posibilidad de suministrar los bienes o prestar los servicios que se requieran; y
- e) El documento que acredite el inicio del trámite o la autorización, en el caso de contrataciones plurianuales.

El estudio de factibilidad será turnado al Órgano Interno de Control respectivo para que, de acuerdo con sus facultades específicas, emita sus sugerencias u observaciones de manera fundada y motivada a través del mismo medio, a más tardar dentro de los 8 días hábiles siguientes a su recepción. Una vez que la DOTIC reciba dicha respuesta podrá enviar el estudio a la Dirección Operativa de Adquisiciones como anexo de la requisición correspondiente.

- V. La DOTIC deberá realizar todos los trámites ante la Unidad de Gobierno Digital de la SFP, en los casos que así lo establezca las disposiciones reglamentarias, obteniendo el Dictamen Técnico favorable de dicha Unidad.

**Artículo 137.-** En las contrataciones relacionadas con los servicios de desarrollo, implementación, soporte a la operación y mantenimiento de aplicativos de cómputo, el Instituto deberá establecer en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o en las solicitudes de cotización, o bien en cualquier otro contrato que se celebre con otros entes públicos, según corresponda, lo siguiente:

- I. Incluir el diseño detallado del aplicativo que se vaya a desarrollar, considerando por lo menos, requerimientos del negocio, de seguridad de la información, de privacidad y protección de datos personales, técnicos, casos de uso, módulos, matriz de trazabilidad y protocolos de pruebas; así como el uso de la Identidad Digital.

Para el desarrollo de aplicativos de cómputo, se deberán indicar las etapas de su participación, así como los objetivos e indicadores de resultado que se espera obtener para las mismas;

- II. Especificar el conjunto de aplicativos de cómputo, en caso de que se prevea utilizar un esquema de tiempo y materiales, debiendo incluir como entregables las bitácoras de actividades del personal que se asigne a tales aplicativos, ya sea desarrollos, implementaciones, soportes a la operación o mantenimientos;

- III. Señalar expresamente, para los aplicativos de cómputo desarrollados con recursos públicos por personal del Instituto o por terceros, que éstos queden bajo la titularidad del Instituto en los términos de la ley aplicable en la materia, en el que se incluirán la totalidad de los componentes del aplicativo de cómputo, como son, el código fuente, el código objeto, el diseño físico y lógico, los manuales técnicos y de usuario;
- IV. Establecer que los aplicativos de cómputo deben ser construidos de forma modular, basados en una Arquitectura Orientada a Servicios, con el objeto de generar aplicaciones reutilizables e interoperables entre diversas áreas del Instituto o con otras instituciones;
- V. Prever que la transferencia, envío y recepción de datos se realice sobre canales seguros en donde se favorezca el cifrado y la integridad de los datos críticos, confidenciales sensibles, en concordancia con las disposiciones referentes a la Seguridad de la Información;
- VI. Requerir, para el caso del desarrollo de aplicativos de cómputo, por lo menos un modelo de tres capas: de datos, del negocio y de presentación;
- VII. Verificar que se cumplan las especificaciones de diseño, codificación y seguridad, definidas por el Instituto, utilizando metodologías o procedimientos estándares para el análisis, diseño, programación y pruebas de los programas informáticos (software) con el objetivo de lograr una mayor confiabilidad, lo cual no deberá ser realizado por el proveedor ni equipo de trabajo que codificó el producto de programas informáticos (software); y
- VIII. En los trámites y servicios digitales que ofrezcan los proveedores, deberán establecer como medio de acreditación personal la Identidad Digital, según resulte procedente. Al efectuar el diseño de aplicativos de cómputo y de servicios nuevos o que requieran de actualizaciones, se implementará la Identidad Digital.

**Artículo 138.-** Con respecto a las redes de telecomunicaciones, el Instituto deberá prever en las convocatorias a la licitación pública o las solicitudes de cotización, que la infraestructura pasiva dentro de las instalaciones del Instituto e incluida en el contrato respectivo quede a favor del Instituto al término de éste.

**Artículo 139.-** En las contrataciones relacionadas con los servicios de Internet, el Instituto deberá prever en las convocatorias a la licitación pública, en las

invitaciones a cuando menos tres personas o las solicitudes de cotización, según corresponda, que los servicios cuenten con lo siguiente:

- I. Mecanismos de protección a ataques de denegación de servicios, desde la propia red del proveedor e independientemente de los controles de seguridad de la información que implemente el Instituto, debiendo atenderse mediante las actividades establecidas en esta Ley, en los controles de seguridad de la información, y
- II. En caso de ser necesario, la distribución y balanceo del tráfico para más de un enlace de Internet, considerando disponibilidad, confidencialidad, criticidad y redundancia.

**Artículo 140.-** En las contrataciones relacionadas con los sistemas de comunicaciones unificadas de telefonía y video, el Instituto deberá prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, según corresponda, que cuenten con lo siguiente:

- I. Prever que la infraestructura pasiva quede a favor del Instituto al término del contrato; y
- II. Maximizar el uso de los sistemas de voz, de video o de ambos, incluidos como parte del servicio, para la elaboración y ejecución conjunta de un plan de adopción tecnológica.

## **Capítulo V**

### **De los procesos de funcionamiento de TIC**

#### **Sección I**

#### **De la implementación**

**Artículo 141.-** La planeación integral del proceso de implementación, incluyendo, si es el caso, la transición de la STSP anterior a la nueva, al menos lo siguiente:

- I. Aseguramiento de suficiencia presupuestal para todo el proceso, multianual si fuese necesario;
- II. Condiciones para modificaciones a la planeación y la suficiencia presupuestal;
- III. Supervisión del cumplimiento del plan de implementación;
- IV. Comprobación de la integridad y funcionalidad de la infraestructura física;
- V. Habilitación de servicios;
- VI. Comprobación de interoperabilidad con las Bases de Datos Nacionales;

- VII. Entidades reguladas por la normativa de Seguridad Privada, configuradas como Fuentes Confiables de Alertamiento;
- VIII. Comprobación de interoperabilidad con las entidades integrantes del Sistema;
- IX. Asignación de perfiles de acceso nominales a las Bases de Datos Nacionales a los integrantes del Sistema;
- X. Asignación de capacidades y facilidades de transferencia nominales a los integrantes del Sistema;
- XI. Capacitación del grupo inicial de personal, conforme a lo dispuesto en capítulo VI del Título Cuarto;
- XII. Prueba Piloto;
- XIII. Prueba Paralelo;
- XIV. Proceso de transición; y
- XV. Definición de normativas para explotación y difusión del contenido de las bases de Datos Nacionales.

## Sección II De la Operación

**Artículo 142.-** El proceso de operación deberá comprender, al menos los siguientes procedimientos:

- I. Proyección medible (indicadores) de objetivos y metas;
- II. EJECUCIÓN, de las actividades requeridas para el logro de los objetivos y metas, sujetas de la evaluación, así como de las necesarias para las adecuaciones derivadas de las modificaciones a la planeación y presupuestación;
- III. Control y seguimiento de las actividades y productividad, tanto en cantidad como en calidad;
- IV. Evaluación del desempeño;
- V. Aseguramiento de suficiencia presupuestal multianual o al menos anual;
- VI. Condiciones para modificaciones a la planeación y la suficiencia presupuestal;
- VII. Supervisión de cumplimiento de objetivos y metas;
- VIII. Aportación obligatoria de datos e información de los integrantes del Sistema de las Bases de Datos de Servicios a las Bases de Datos Nacionales;
- IX. Autonomía funcional para operación de las responsabilidades institucionales y servicios;
- X. Administración de integración y acceso de contenido de las Bases de Datos Nacionales;
- XI. Ampliación de perfiles de acceso nominales a las Bases de Datos Nacionales a los integrantes del Sistema bajo indicaciones puntuales;
- XII. Acceso restringido a las Bases de Datos Nacionales;

- XIII. Acceso directo a las Bases de Datos Nacionales, por parte de los integrantes del Sistema;
- XIV. Ampliación de capacidades y facilidades de transferencia nominales a los integrantes del Sistema bajo indicaciones puntuales;
- XV. Capacitación inicial para personal de nuevo ingreso, conforme a lo dispuesto en capítulo VI del Título Cuarto;
- XVI. Capacitación de conservación de competencias laborales, conforme a lo dispuesto en capítulo VI del Título Cuarto; y
- XVII. Cumplimiento de normativas para explotación y difusión del contenido de las bases de Datos Nacionales.

### **Sección III De la Conservación y Mantenimiento**

**Artículo 143.-** El proceso de conservación y mantenimiento, comprende al menos los siguientes procedimientos:

- I. Proyección medible (indicadores) de objetivos y metas;
- II. Ejecución de las actividades para el logro de los objetivos y metas;
- III. Control de la productividad, tanto en cantidad como en calidad;
- IV. Evaluación del desempeño;
- V. Aseguramiento de suficiencia presupuestal. multianual o al menos anual;
- VI. Condiciones para modificaciones a la planeación y la suficiencia presupuestal;
- VII. Supervisión de cumplimiento de objetivos y metas;
- VIII. Mecanismos de Seguridad de la Información para la protección y salvaguarda de contenidos en almacenamiento y transferencias (cadena de custodia) en las Bases de Datos de Servicios;
- IX. Aseguramiento de la continuidad funcional del acervo de TIC;
- X. Mecanismos de Seguridad de la Información para la protección y salvaguarda de contenidos en almacenamiento y transferencias (cadena de custodia) en las Bases de Datos Nacionales; y
- XI. Actualización de modelos y contenidos de capacitación.

## **TITULO SEXTO DE LAS FALTAS ADMINISTRATIVAS DE LOS USUARIOS Y DE LAS RESPONSABILIDADES DE LOS SERVIDORES PÚBLICOS**

### **Capítulo I De las Faltas Administrativas y de los Delitos**

**Artículo 144.-** Cometan infracciones a lo dispuesto por esta ley, quienes en calidad de usuarios del Sistema:

- I. **Suministren datos falsos, incompletos o incongruentes;**
- II. **Realicen llamadas o avisos falsos o de broma;**
- III. **Inicien llamadas de emergencia o avisos de cualquier naturaleza y los interrumpan intencionalmente, proporcionando información falsa, falaz o con fines de distracción de las tareas de la autoridad;**
- IV. **Impidan el acceso al evento de emergencia a las corporaciones de auxilio prestadoras del servicio;**
- V. **Interfieran de cualquier forma la prestación de los servicios de las corporaciones de auxilio.**
- VI. **Incumplimiento de normativas de aportación, acceso y difusión de información de las Bases de Datos Nacionales**

**Artículo 145.- Se sancionará en los términos de los tipos penales de acuerdo con las leyes en la materia correspondientes, a quienes:**

- I. **Ingresen, sin motivo justificado y sin autorización de quien deba proporcionarla, a las Bases de Datos del Sistema, con fines comerciales o de sabotaje informático; y**
- II. **Divulguen de manera ilícita información clasificada de las bases de datos o de los sistemas informáticos del Sistema a que se refiere esta ley.**

**Artículo 146.- Las faltas administrativas se sancionarán conforme a los Reglamentos o Bandos de Policía y Gobierno o análogos.**

## **Capítulo II**

### **De las Responsabilidades de los Servidores Públicos**

**Artículo 147.- Son responsabilidades imputables a los servidores públicos del Instituto, las siguientes:**

- I. **La revelación de datos confidenciales;**
- II. **La revelación de los datos proporcionados por los usuarios, en contra de lo dispuesto por esta ley y las demás disposiciones aplicables;**
- III. **La utilización de los sistemas informáticos y de las bases de datos para fines distintos a los previstos en esta ley;**

**IV. Permitir y colaborar con personas ajenas al servicio público, en la violación de las bases de datos del Sistema.**

**Artículo 148.- Las sanciones a los servidores públicos serán las establecidas en la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos y, en su caso, por las disposiciones en materia penal.**

**Artículo Segundo.** – Se adiciona la fracción VI, recorriéndose en su orden las subsecuentes, se reforma la actual fracción XVII recorrida como fracción XVIII del artículo 5; se reforma el primer párrafo del artículo 17; se deroga el artículo 19; se reforma la denominación del Título Séptimo; y se reforma el artículo 109 bis en su primer párrafo y en su fracción V, de la Ley General del Sistema Nacional de Seguridad Pública, para quedar como sigue:

**Artículo 5 ...**

- I. ...
- II. ...
- III. ...
- IV. ...
- V. ...

**VI. Centro Nacional de Información: al Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública.**

**VII. Conferencias Nacionales:** a las Conferencias a las que se refiere el artículo 10 de esta Ley;

**VIII. Consejo Nacional:** al Consejo Nacional de Seguridad Pública;

**IX. Instituciones de Seguridad Pública:** a las Instituciones Policiales, de Procuración de Justicia, del Sistema Penitenciario y dependencias encargadas de la Seguridad Pública a nivel federal, local y municipal;

**X. Instituciones de Procuración de Justicia:** a las Instituciones de la Federación y entidades federativas que integran al Ministerio Público, los servicios periciales, policías de investigación y demás auxiliares de aquel;

**XI. Instituciones Policiales:** a los cuerpos de policía, de vigilancia y custodia de los establecimientos penitenciarios, de detención preventiva, o de centros de arraigos; y en general, todas las dependencias encargadas de la seguridad pública a nivel federal, local y municipal, que realicen funciones similares;

**XII. Institutos:** a los órganos de las instituciones de seguridad pública de la Federación, de los Estados y del Distrito Federal, encargados de la formación y

actualización especializada de aspirantes y servidores públicos de las funciones ministerial, pericial y de policía ministerial;

**XIII.** Programa Rector: al conjunto de contenidos encaminados a la profesionalización de los servidores públicos de las Instituciones Policiales e Instituciones de Procuración de Justicia, respectivamente;

**XIV.** Registro Nacional: el Registro Nacional de Personal de las Instituciones de Seguridad Pública;

**XV.** Secretaría: a la Secretaría de Seguridad y Protección Ciudadana del Gobierno Federal;

**XVI.** Secretario Ejecutivo: el Titular del Secretariado Ejecutivo del Sistema;

**XVII.** Sistema: al Sistema Nacional de Seguridad Pública, y

**XVIII.** Sistema Nacional de Información: al Sistema Nacional de **la Información y Comunicaciones para la Seguridad Pública, a que se refiere la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública.**

**Artículo 17.-** El Secretariado Ejecutivo es el órgano operativo del Sistema y gozará de autonomía técnica, de gestión y presupuestal. Contará con los **Centros Nacionales de Prevención del Delito y Participación Ciudadana**, así como de Certificación y Acreditación. El Titular del Ejecutivo Federal expedirá el Reglamento del Secretariado, que establecerá las atribuciones y articulación de estos Centros.

...

I ...

II ...

III ...

IV ...

V ...

**Artículo 19.- Derogado.**

## TÍTULO SÉPTIMO

### DEL SISTEMA NACIONAL DE LA INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD PÚBLICA

**Artículo 109 Bis. - El Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública** será la encargada de la operación de la plataforma tecnológica que sustenta el Sistema Nacional de Información, a través de la unidad administrativa que su titular determine. Dicha unidad tendrá, entre otras, las siguientes atribuciones:

I. ...

II. ...

III. ...

IV. ...

**V. Proponer el Plan Anual de Desarrollo y Modernización Tecnológica** al Consejo Nacional de Seguridad Pública;

VI. ...

VII. ...

VIII. ...

**Artículo Tercero. –** Se adiciona un último párrafo al artículo 33 de la Ley del Sistema Nacional de Información Estadística y Geográfica, para quedar como sigue:

**ARTÍCULO 33.- ...**

I a la VII ...

...

...

**El Instituto Nacional de la Información y Comunicaciones para la Seguridad Pública determinará las normas relativas a la información que produzca y requiera, en materia de seguridad pública, sin menoscabo de participar en los comités: ejecutivo y técnico especializado, que corresponda para la debida coordinación con el INEGI.**

**Artículo Cuarto. –** Se reforman las fracciones XXIV y XL del artículo 9 de la Ley de la Guardia Nacional, para quedar como sigue:

Artículo 9. ...

I a la XXIII...

**XXIV.** Incorporar a las Bases de Datos del Sistema Nacional de **la Información y Comunicaciones para la Seguridad Pública, con estricto apego a las normas establecidas al efecto por el Instituto Nacional del Sistema de Información y Comunicaciones para la Seguridad Pública** la información que pueda ser útil en la investigación de los delitos y utilizar su contenido para el desempeño de sus atribuciones, sin afectar el derecho de las personas a la protección de sus datos personales;

XXV a XXXIX. ...

**XL.** Integrar al Sistema Nacional de **la Información y Comunicaciones para la Seguridad Pública con estricto apego a las normas establecidas al efecto por el Instituto Nacional del Sistema de Información y Comunicaciones para la Seguridad Pública** los datos que se recaben para identificar a las personas;

XLI a la XLIV. ...

**Artículo Quinto.** – Se reforma el inciso a., de la fracción VIII del artículo 26 de la Ley Orgánica de la Fiscalía General de la República, para quedar como sigue:

Artículo 26. ...

I a la VIII. ...

- a. El intercambio de información, documentación, bases de datos, a través de sistemas de interoperabilidad, **particularmente con el Instituto Nacional del Sistema de la Información y Comunicaciones para la Seguridad Pública respecto de la información que en su caso puedan requerir las bases de datos nacionales del Sistema Nacional de Seguridad Pública, así como las**

**necesarias para la integración de las estadísticas de incidencia delictiva del orden federal;**

b. ...

c. ...

d. ...

e. ...

f. ...

IX a la X. ...

**Artículo Sexto.** – Se adiciona la fracción XXVIII recorriéndose en su orden las subsecuentes del artículo 3 y se reforma la fracción XII del artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, para quedar como sigue:

Artículo 3. ...

I. a la XXVII. ...

**XXVIII.- Instancias de Seguridad o Instancias de Seguridad y Procuración de Justicia. - Comprende a las Instituciones de Seguridad Pública a que se refiere la fracción VIII del artículo 5 de Ley General del Sistema Nacional de Seguridad Pública y al Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública de la Ley Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;**

**XXIX. Instituto: Instituto Federal de Telecomunicaciones;**

**XXX.** Insumos esenciales: Elementos de red o servicios que se proporcionan por un solo concesionario o un reducido número de concesionarios, cuya reproducción no es viable desde un punto de vista técnico, legal o económico y son insumos indispensables para la prestación de los servicios de telecomunicaciones y de radiodifusión. En los casos no previstos en esta Ley, el Instituto determinará la existencia y regulación al acceso de insumos esenciales en términos de lo dispuesto por la Ley Federal de Competencia Económica;

**XXXI.** Interconexión: Conexión física o virtual, lógica y funcional entre redes públicas de telecomunicaciones que permite la conducción de tráfico entre dichas redes y/o entre servicios de telecomunicaciones prestados a través de las mismas, de manera que los usuarios de una de las redes públicas de telecomunicaciones puedan conectarse e intercambiar tráfico con los usuarios de otra red pública de telecomunicaciones y viceversa, o bien permite a los usuarios de una red pública de telecomunicaciones la utilización de servicios de telecomunicaciones provistos por o a través de otra red pública de telecomunicaciones;

**XXXII.** Interferencia perjudicial: Efecto de una energía no deseada debida a una o varias emisiones, radiaciones, inducciones o sus combinaciones sobre la recepción en un sistema de telecomunicaciones o radiodifusión, que puede manifestarse como degradación de la calidad, falseamiento o pérdida de información, que compromete, interrumpe repetidamente o impide el funcionamiento de cualquier servicio de radiocomunicación;

**XXXIII.** Internet: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única;

**XXXIV.** Interoperabilidad: Características técnicas de las redes públicas, sistemas y equipos de telecomunicaciones integrados a éstas que permiten la interconexión efectiva, por medio de las cuales se asegura la provisión de un servicio de telecomunicaciones específico de una manera consistente y predecible, en términos de la entrega funcional de servicios entre redes;

**XXXV.** Ley: Ley Federal de Telecomunicaciones y Radiodifusión;

**XXXVI.** Localización geográfica en tiempo real: Es la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada;

**XXXVII.** Mensaje Comercial: Mención dirigida al público o a un segmento del mismo durante corte programático, con el propósito de informar sobre la existencia o características de un producto, servicio o actividad para inducir su comercialización y venta, en las estaciones de radiodifusión con concesión comercial y canales de televisión y audio restringidos. El mensaje comercial no incluye los promocionales propios de la estación o canal, ni las transmisiones correspondientes a los tiempos del Estado, y otros a disposición del Poder Ejecutivo, ni programas de oferta de productos y servicios;

**XXXVIII.** Multiprogramación: Distribución de más de un canal de programación en el mismo canal de transmisión;

**XXXIX.** Neutralidad a la competencia: Obligación del Estado de no generar distorsiones al mercado como consecuencia de la propiedad pública;

**XL.** Órbita satelital: Trayectoria que recorre una estación espacial alrededor de la Tierra;

**XLI.** Patrocinio: El pago en efectivo o en especie que realiza cualquier persona física o moral a fin de que se haga la mención o presentación visual de la denominación, razón social, marca o logotipo de la persona que realizó el pago;

**XLII.** Películas cinematográficas: Creación audiovisual compuesta por imágenes en movimiento, con o sin sonorización incorporada, con una duración de sesenta minutos o superior. Son películas nacionales las realizadas por personas físicas o morales mexicanas o las realizadas en el marco de los acuerdos internacionales o los convenios de coproducción suscritos por el gobierno mexicano, con otros países u organismos internacionales;

**XLIII. Poder de mando:** La capacidad de hecho de influir de manera decisiva en los acuerdos adoptados en las asambleas de accionistas o sesiones del consejo de administración o en la gestión, conducción y ejecución de los negocios de una persona que ésta controle o en las que tenga una influencia significativa;

**XLIV. Política de inclusión digital universal:** Conjunto de programas y estrategias emitidos por el Ejecutivo Federal orientadas a brindar acceso a las tecnologías de la información y la comunicación, incluyendo el Internet de banda ancha para toda la población, haciendo especial énfasis en sus sectores más vulnerables, con el propósito de cerrar la brecha digital existente entre individuos, hogares, empresas y áreas geográficas de distinto nivel socioeconómico, respecto a sus oportunidades de acceso a las tecnologías referidas y el uso que hacen de éstas;

**XLV. Portabilidad:** Derecho de los usuarios de conservar el mismo número telefónico al cambiarse de concesionario o prestador de servicio;

**XLVI. Posiciones orbitales geoestacionarias:** Ubicaciones en una órbita circular que se encuentran en el plano ecuatorial, que permiten que un satélite mantenga un periodo de traslación igual al periodo de rotación de la Tierra;

**XLVII. Preponderancia:** Calidad determinada por el Instituto de un agente económico en los términos del artículo 262 de esta Ley;

**XLVIII. Producción nacional:** Contenido o programación generada por persona física o moral con financiamiento mayoritario de origen mexicano;

**XLIX. Productor nacional independiente de contenidos audiovisuales:** Persona física o moral de nacionalidad mexicana que produce obras audiovisuales a nivel nacional, regional o local, que no cuenta con una concesión de telecomunicaciones o radiodifusión, ni es controlado por un concesionario en virtud de su poder de mando;

**L. PROFECO:** La Procuraduría Federal del Consumidor;

**LI. Programación de oferta de productos:** La que, en el servicio de radio y televisión tiene por objeto ofrecer o promover la venta de bienes o la prestación de servicios y cuya duración es superior a cinco minutos continuos;

**LII. Programador nacional independiente:** Persona física o moral que no es objeto de control por parte de algún concesionario de radiodifusión o por alguna afiliada, filial o subsidiaria de éste, ni es controlado por un concesionario en virtud de su poder de mando, que cuenta con la capacidad de conformar un canal de programación con base en estructura programática formada mayoritariamente por producción propia y producción nacional independiente y cuya titularidad sobre los derechos de autor sea mayoritariamente mexicana;

**LIII. Punto de interconexión:** Punto físico o virtual donde se establece la interconexión entre redes públicas de telecomunicaciones para el intercambio de tráfico de interconexión o de tráfico de servicios mayoristas;

**LIV. Radiocomunicación:** Toda telecomunicación o radiodifusión que es transmitida por ondas del espectro radioeléctrico;

**LV. Radiodifusión:** Propagación de ondas electromagnéticas de señales de audio o de audio y video asociado, haciendo uso, aprovechamiento o explotación de las bandas de frecuencia del espectro radioeléctrico, incluidas las asociadas a recursos orbitales, atribuidas por el Instituto a tal servicio, con el que la población puede recibir de manera directa y gratuita las señales de su emisor utilizando los dispositivos idóneos para ello;

**LVI. Recursos orbitales:** Posiciones orbitales geoestacionarias u órbitas satelitales con sus respectivas bandas de frecuencias asociadas que pueden ser objeto de concesión;

**LVII. Red compartida mayorista:** Red pública de telecomunicaciones destinada exclusivamente a comercializar capacidad, infraestructura o servicios de telecomunicaciones al mayoreo a otros concesionarios o comercializadoras;

**LVIII. Red de telecomunicaciones:** Sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro

radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;

**LIX.** Red pública de telecomunicaciones: Red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios, ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;

**LX.** Satélite: Objeto colocado en una órbita satelital, provisto de una estación espacial con sus frecuencias asociadas que le permite recibir, transmitir o retransmitir señales de radiocomunicación desde o hacia estaciones terrenas u otros satélites;

**LXI.** Secretaría: La Secretaría de Comunicaciones y Transportes;

**LXII.** Servicio de usuario visitante: El servicio a través del cual los usuarios de una red pública de telecomunicaciones de servicio local móvil, pueden originar o recibir comunicaciones de voz o datos a través de la infraestructura de acceso de otro concesionario de red pública de telecomunicaciones del servicio local móvil, sin necesidad de realizar algún procedimiento adicional, al tratarse de usuarios de otra región local móvil o al estar fuera de la zona de cobertura de su proveedor de servicios móviles;

**LXIII.** Servicio mayorista de telecomunicaciones: Servicio de telecomunicaciones que consiste en el suministro de acceso a elementos individuales, a capacidades de una red o servicios, incluyendo los de interconexión, que son utilizados por concesionarios o comercializadores para proveer servicios de telecomunicaciones a los usuarios finales;

**LXIV.** Servicios de interconexión: Los que se prestan entre concesionarios de servicios de telecomunicaciones, para realizar la interconexión entre sus redes e incluyen, entre otros, la conducción de tráfico, su originación y terminación, enlaces de transmisión, señalización, tránsito, puertos de acceso, ubicación, la compartición de infraestructura para interconexión, facturación y cobranza, así como otros servicios auxiliares de la misma y acceso a servicios;

**LXV.** Servicio de televisión y audio restringidos: Servicio de telecomunicaciones de audio o de audio y video asociados que se presta a suscriptores, a través de redes públicas de telecomunicaciones, mediante contrato y el pago periódico de una cantidad preestablecida;

**LXVI.** Servicios públicos de telecomunicaciones y radiodifusión: Servicios de interés general que prestan los concesionarios al público en general con fines comerciales, públicos o sociales de conformidad con lo dispuesto en la presente Ley y la Ley Federal de Competencia Económica;

**LXVII.** Sistema de comunicación por satélite: El que permite el envío de señales de radiocomunicación a través de una estación terrena transmisora a un satélite que las recibe, amplifica, procesa y envía de regreso a la Tierra para ser captada por una o varias estaciones terrenas receptoras;

**LXVIII.** Sitio público: Para efectos de esta Ley y siempre que se encuentren a cargo de dependencias o entidades federales, estatales o municipales o bajo programas públicos de cualquiera de los tres órdenes de gobierno, se consideran como tal a:

- a. Escuelas, universidades y, en general, inmuebles destinados a la educación;
- b. Clínicas, hospitales, centros de salud y, en general, inmuebles para la atención de la salud;
- c. Oficinas de los distintos órdenes de gobierno;
- d. Centros comunitarios;
- e. Espacios abiertos tales como plazas, parques, centros deportivos y áreas públicas de uso común para la población en general, cuya construcción o conservación está a cargo de autoridades federales, estatales, municipales o del Distrito Federal;

f. Aquellos que participen en un programa público, y

g. Los demás que se consideren sitios públicos de acuerdo a la legislación vigente;

**LXIX.** Telecomunicaciones: Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión;

**LXX.** Tráfico: Datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que circulan por una red de telecomunicaciones;

**LXXI.** Valor mínimo de referencia: Cantidad expresada en dinero, misma que será considerada como el valor mínimo que se deberá pagar como contraprestación por la adjudicación de la concesión, y

**LXXII.** Usuario final: Persona física o moral que utiliza un servicio de telecomunicaciones como destinatario final.

...

**Artículo 190. ...**

I a la XI. ...

**XII.** Realizar bajo la coordinación del Instituto, **y en su caso, con la colaboración del Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública** los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Los concesionarios que operen redes públicas de telecomunicaciones podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e

investigaciones. Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Instituto, al Congreso de la Unión y al Ejecutivo Federal.

...

**Artículo Séptimo.** – Se adiciona la fracción XXXVI, recorriéndose en su orden las subsecuentes del artículo 2; se reforma el segundo párrafo del artículo 16; se adiciona la fracción XXXI recorriéndose en su orden las subsecuentes del artículo 19; se adiciona un párrafo al artículo 21 recorriéndose las subsecuentes, y se adiciona un segundo párrafo al artículo 24 recorriéndose las subsecuentes de la Ley General de Protección Civil, para quedar como sigue:

Artículo 2. ...

I. a la XXXV. ...

**XXXVI. ISINISP.- Instituto Nacional del Sistema Nacional de la Información y Comunicaciones para la Seguridad Pública;**

**XXXVII. Mitigación:** Es toda acción orientada a disminuir el impacto o daños ante la presencia de un agente perturbador sobre un agente afectable;

**XXXVIII. Peligro:** Probabilidad de ocurrencia de un agente perturbador potencialmente dañino de cierta intensidad, durante un cierto periodo y en un sitio determinado;

**XXXIX. Preparación:** Actividades y medidas tomadas anticipadamente para asegurar una respuesta eficaz ante el impacto de un fenómeno perturbador en el corto, mediano y largo plazo;

**XL. Prevención:** Conjunto de acciones y mecanismos implementados con antelación a la ocurrencia de los agentes perturbadores, con la finalidad de conocer los peligros o los riesgos, identificarlos, eliminarlos o reducirlos; evitar o mitigar su impacto destructivo sobre las personas, bienes, infraestructura, así como anticiparse a los procesos sociales de construcción de los mismos

**XLII.** Previsión: Tomar conciencia de los riesgos que pueden causarse y las necesidades para enfrentarlos a través de las etapas de identificación de riesgos, prevención, mitigación, preparación, atención de emergencias, recuperación y reconstrucción;

**XLIII.** Programa Interno de Protección Civil: Es un instrumento de planeación y operación, circunscrito al ámbito de una dependencia, entidad, institución u organismo del sector público, privado o social; que se compone por el plan operativo para la Unidad Interna de Protección Civil, el plan para la continuidad de operaciones y el plan de contingencias, y tiene como propósito mitigar los riesgos previamente identificados y definir acciones preventivas y de respuesta para estar en condiciones de atender la eventualidad de alguna emergencia o desastre;

**XLIV.** Programa Nacional: Al Programa Nacional de Protección Civil;

**XLV.** Protección Civil: Es la acción solidaria y participativa, que en consideración tanto de los riesgos de origen natural o antrópico como de los efectos adversos de los agentes perturbadores, prevé la coordinación y concertación de los sectores público, privado y social en el marco del Sistema Nacional, con el fin de crear un conjunto de disposiciones, planes, programas, estrategias, mecanismos y recursos para que de manera corresponsable, y privilegiando la Gestión Integral de Riesgos y la Continuidad de Operaciones, se apliquen las medidas y acciones que sean necesarias para salvaguardar la vida, integridad y salud de la población, así como sus bienes; la infraestructura, la planta productiva y el medio ambiente;

**XLVI.** Reconstrucción: La acción transitoria orientada a alcanzar el entorno de normalidad social y económica que prevalecía entre la población antes de sufrir los efectos producidos por un agente perturbador en un determinado espacio o jurisdicción. Este proceso debe buscar en la medida de lo posible la reducción de los riesgos existentes, asegurando la no generación de nuevos riesgos y mejorando para ello las condiciones preexistentes;

**XLVII.** Recuperación: Proceso que inicia durante la emergencia, consistente en acciones encaminadas al retorno a la normalidad de la comunidad afectada;

**XLVIII.** Reducción de Riesgos: Intervención preventiva de individuos, instituciones y comunidades que nos permite eliminar o reducir, mediante acciones de preparación

y mitigación, el impacto adverso de los desastres. Contempla la identificación de riesgos y el análisis de vulnerabilidades, resiliencia y capacidades de respuesta, el desarrollo de una cultura de la protección civil, el compromiso público y el desarrollo de un marco institucional, la implementación de medidas de protección del medio ambiente, uso del suelo y planeación urbana, protección de la infraestructura crítica, generación de alianzas y desarrollo de instrumentos financieros y transferencia de riesgos, y el desarrollo de sistemas de alertamiento;

**XLVIII. Refugio Temporal:** La instalación física habilitada para brindar temporalmente protección y bienestar a las personas que no tienen posibilidades inmediatas de acceso a una habitación segura en caso de un riesgo inminente, una emergencia, siniestro o desastre

**XLIX. Resiliencia:** Es la capacidad de un sistema, comunidad o sociedad potencialmente expuesta a un peligro para resistir, asimilar, adaptarse y recuperarse de sus efectos en un corto plazo y de manera eficiente, a través de la preservación y restauración de sus estructuras básicas y funcionales, logrando una mejor protección futura y mejorando las medidas de reducción de riesgos;

**L. Riesgo:** Daños o pérdidas probables sobre un agente afectable, resultado de la interacción entre su vulnerabilidad y la presencia de un agente perturbador;

**LI. Riesgo Inminente:** Aquel riesgo que, según la opinión de una instancia técnica especializada, debe considerar la realización de acciones inmediatas en virtud de existir condiciones o altas probabilidades de que se produzcan los efectos adversos sobre un agente afectable;

**LII. Secretaría:** La Secretaría de Gobernación del Gobierno Federal;

**LIII. Seguro:** Instrumento de Administración y Transferencia de Riesgos;

**LIV. Simulacro:** Representación mediante una simulación de las acciones de respuesta previamente planeadas con el fin de observar, probar y corregir una respuesta eficaz ante posibles situaciones reales de emergencia o desastre. Implica el montaje de un escenario en terreno específico, diseñado a partir de la identificación y análisis de riesgos y la vulnerabilidad de los sistemas afectables;

**LV. Sistema Nacional:** El Sistema Nacional de Protección Civil;

**LVI. Siniestro:** Situación crítica y dañina generada por la incidencia de uno o más fenómenos perturbadores en un inmueble o instalación afectando a su población y equipo, con posible afectación a instalaciones circundantes;

**LVII. Unidad Interna de Protección Civil:** El órgano normativo y operativo responsable de desarrollar y dirigir las acciones de protección civil, así como elaborar, actualizar, operar y vigilar el Programa Interno de Protección Civil en los inmuebles e instalaciones fijas y móviles de una dependencia, institución o entidad perteneciente a los sectores público, privado y social; también conocidas como Brigadas Institucionales de Protección Civil;

**LVIII. Unidades de Protección Civil:** Los organismos de la administración pública de las entidades federativas, municipales o de las delegaciones, encargados de la organización, coordinación y operación del Sistema Nacional, en su demarcación territorial;

**LIX. Vulnerabilidad:** Susceptibilidad o propensión de un agente afectable a sufrir daños o pérdidas ante la presencia de un agente perturbador, determinado por factores físicos, sociales, económicos y ambientales;

**LX. Zona de Desastre:** Espacio territorial determinado en el tiempo por la declaración formal de la autoridad competente, en virtud del desajuste que sufre en su estructura social, impidiéndose el cumplimiento normal de las actividades de la comunidad. Puede involucrar el ejercicio de recursos públicos a través del Fondo de Desastres;

**LXI. Zona de Riesgo:** Espacio territorial determinado en el que existe la probabilidad de que se produzca un daño, originado por un fenómeno perturbador, y

**LXII. Zona de Riesgo Grave:** Asentamiento humano que se encuentra dentro de una zona de grave riesgo, originado por un posible fenómeno perturbador.

Artículo 16. ...

Los integrantes del Sistema Nacional deberán compartir con la autoridad competente que solicite y justifique su utilidad, la información de carácter técnico, ya sea impresa, electrónica o en tiempo real relativa a los sistemas y/o redes de alerta, detección, monitoreo, pronóstico y medición de riesgos. **En especial el ISINISP y los Complejos de Seguridad compartirán con el Sistema Nacional la información sobre emergencias que reciban, cuando impliquen la atención de dicho Sistema.**

Artículo 19. ...

I, a la XXX. ...

**XXXI.- Establecer las bases de coordinación con el ISINISP, para los servicios que prestan los Centros de Supervisión y Control Regional de ese Instituto y los Complejos de Seguridad de las Entidades Federativas;**

**XXXII.** Las demás que señalen los ordenamientos aplicables o que le atribuyan el Presidente o el Consejo Nacional dentro de la esfera de sus facultades.

Artículo 21. ...

...

**Se atenderán los avisos de emergencia recibidos por los Complejos de Seguridad de la Entidades Federativas, de acuerdo con las bases establecidas conforme a la fracción XXXI del artículo 19 de esta Ley.**

...

...

...

...

## Artículo 24. ...

Recibirá y atenderá de manera prioritaria los avisos de emergencia de los Complejos de Seguridad de las Entidades Federativas, recibidos por estas instancias, determinando en primer lugar si dicha emergencia corresponde a la atención del Sistema o a otras instancias de atención de emergencias, incluyendo la de seguridad pública y, en su caso, procederá a su inmediato alertamiento a las instancias correspondientes del Sistema.

## TRANSITORIOS

**PRIMERO.** El presente Decreto entrará en vigor al día siguiente del de su publicación en el Diario Oficial de la Federación, salvo en lo previsto en los artículos transitorios siguientes.

**SEGUNDO.** La designación de los primeros integrantes de la Junta de Gobierno del Instituto se realizará bajo los términos previstos en la presente Ley, dentro de los 30 días naturales siguientes a la publicación de esta en el Diario Oficial de la Federación.

La designación del primer director general se realizará dentro de los 30 días naturales siguientes a la publicación de la presente Ley.

El periodo del primer director general del Instituto vencerá el 30 de noviembre de 2021.

**TERCERO.** El Instituto Nacional del Sistema de Información y Comunicaciones para la Seguridad Pública, tendrá la titularidad de todos los bienes, derechos y obligaciones propiedad del gobierno federal que estuvieran adscritos o destinados bajo cualquier título al servicio del Centro Nacional de Información del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y del Centro de Información Plataforma México, ambos de la Secretaría de Seguridad y Protección Ciudadana.

**CUARTO.** Los recursos humanos, materiales y financieros con que cuenten el Centro Nacional de Información del Secretariado Ejecutivo del Sistema Nacional

de Seguridad Pública y del Centro de Información Plataforma México, ambos de la Secretaría de Seguridad y Protección Ciudadana, se transferirán al Instituto, dentro de los 60 días naturales siguientes a la publicación de esta Ley.

**QUINTO.** El Ejecutivo Federal expedirá las disposiciones reglamentarias de la presente Ley en un plazo no mayor a 12 meses a partir de la entrada en vigor de este decreto.

**SEXTO.** El Gobierno Federal, a través de la Secretaría de Hacienda y Crédito Público, deberá realizar las ampliaciones presupuestales necesarias para el cumplimiento de la presente Ley en el presente ejercicio y establecer las partidas presupuestales específicas en el Presupuesto de Egresos de la Federación para el siguiente ejercicio fiscal a su entrada en vigor.

**SEPTIMO.** Se derogarán todas las disposiciones legales de las Leyes de las entidades federativas que se opongan al presente decreto.

**OCTAVO.** El Gobierno Federal, dentro de los 180 días siguientes a la entrada en vigor del presente decreto, deberá realizar las adecuaciones necesarias a las disposiciones aplicables en la materia, que se relacionen con las Leyes vinculadas con este decreto.

**NOVENO.** El Gobierno Federal, en el ámbito de sus atribuciones en un periodo no mayor a 90 días a partir de la entrada en vigor del presente decreto, deberá realizar las acciones necesarias y llevar a cabo los actos jurídicos y administrativos a que se refieren las disposiciones de los artículos transitorios tercero y cuarto.

**DÉCIMO.** La Junta de Gobierno del Instituto deberá aprobar dentro de los 180 días siguientes a la publicación del presente decreto el Reglamento Interno y el Manual de Organización General del Instituto.

**DÉCIMO PRIMERO.** El Instituto dentro de los 360 días, contados a partir de la entrada en vigor del presente decreto, deberá realizar el inventario y diagnóstico de la infraestructura de TIC y de comunicaciones, así como el programa de regularización de las mismas.

Palacio Legislativo de San Lázaro, a 01 de julio de 2020

Diputado Moisés Ignacio Mier Velazco.